

Discussierapport

GRC in de bouw aan de maat?

Ontwikkelingen in de bouwsector
op het gebied van governance,
risicomanagement en compliance

Nederlandse
Beroepsorganisatie
van Accountants

NBA



Eindredactie

San Croonenberg

Klankbordgroep

CFO RWS - Richard van Breukelen

Voorzitter Bouwend Nederland - Elco Brinkman

Directeur Vernieuwing Bouw - Jacqueline Schlangen

Partner KPMG, Internal Audit, Risk & Compliance Services - Bart van Loon

Opdrachtgever

Ledengroep Intern en Overheidsaccountants (LIO) van de NBA. Eindverantwoordelijk bestuurslid: Paul Scholte

Projectgroep

San Croonenberg, projectleider

Joop Brakenhoff, projectlid

Eddy van der Geest, projectlid

Michael Schoevaart, projectlid

Heiko van der Wijk, projectlid

Copyright © 2012 NBA, Amsterdam. Overname van (gedeelten van) de tekst is toegestaan onder bronvermelding. Grafische verzorging: NBA

Inhoudsopgave

| | | |
|----|---|----|
| 1. | Samenvatting | 5 |
| 2. | GRC-speelveld en achtergrond in het kort | 7 |
| 3. | Discussiepunten | 9 |
| 4. | Good practices | 11 |
| 5. | GRC in de bouw | 13 |
| | 5.1. Governance | 14 |
| | 5.2. Risicomanagement | 15 |
| | 5.3. Compliance | 16 |
| 6. | Aanleiding en werkwijze onderzoek | 19 |
| | 6.1. Aanleiding | 19 |
| | 6.2. Werkwijze onderzoek | 20 |
| 7. | GRC-ontwikkeling en uitleg model | 21 |
| | Bijlage 1 - Geraadpleegde modellen, artikelen, onderzoeken en links naar websites | 23 |
| | Bijlage 2 - Afkortingenlijst | 25 |
| | Bijlage 3 - GRC-normenkader voor de bouwsector | 26 |

Voorwoord

Voor u ligt een lezenswaardig rapport waarin de mate van ontwikkeling van Governance, Risicomanagement en Compliance (GRC) bij grote Nederlandse bouwondernemingen is onderzocht. Ik beveel u dit rapport van harte aan omdat ik van mening ben dat het een bijdrage kan leveren aan het verder professionaliseren van het GRC-speelveld en daarmee aan de verbetering van de interne beheersing en bedrijfsvoering in het algemeen en de kwaliteit van het toezicht daarop in het bijzonder.

Dat is temeer belangrijk omdat de afgelopen jaren veel te doen is geweest in en rondom de bouwsector. Normen voor governance, transparantie en integriteit worden helderder bij een veranderende markt door samenwerking bij toepassing van geïntegreerde contracten. GRC is in dit kader nog lang niet uitgekristalliseerd en zowel opdrachtgevers als opdrachtnemers hebben nog een weg te gaan.

Regelgeving is stringenter geworden en er zijn verwachtingen gewekt bij het maatschappelijk verkeer waarvan de resultaten beneden de maat zijn gebleven. Het vertrouwen in bouworganisaties, bestuurders en toezichthouders heeft daardoor te lijden gehad. Het is voor iedereen van groot belang dat het vertrouwen wordt hersteld en dat bouwondernemingen weer een goede reputatie krijgen. De aanbeveling uit dit rapport en de good practices kunnen daarbij, naar mijn stellige overtuiging, als leidraad dienen.

drs. Ingrid Doerga RA

Voorzitter bestuur Ledengroep Intern en Overheidsaccountants
van de Nederlandse Beroepsorganisatie van Accountants

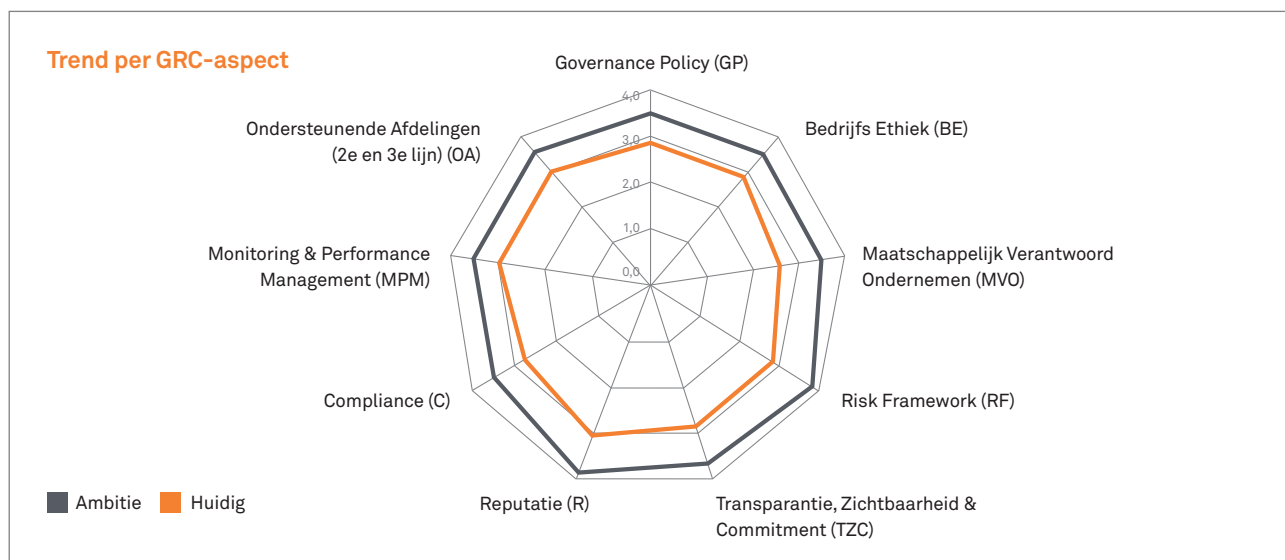
01 | Samenvatting

Aanleiding

Hedendaagse dynamiek en onzekerheden over economische ontwikkelingen dwingen ondernemingen tot een sterkere en effectievere beheersing en monitoring van hun processen. Eisen en verplichtingen, maar vooral verwachtingen uit regelgeving en maatschappij nemen toe. Maatschappelijk verantwoord ondernemen behoort nu tot een vanzelfsprekende voorwaarde. Dit geldt onverkort voor de bouwsector en aanverwante ondernemingen.

Samenvattende uitkomsten

Dit rapport beschrijft de resultaten van het onderzoek naar ontwikkelingen op het gebied van governance, risicomanagement en compliance (GRC) bij grote bouwondernemingen en aanverwante industrie in Nederland. Met behulp van een self-assessment vragenlijst zijn de ondernemingen gevraagd hun huidige en geambieerde ontwikkelingsfasen aan te geven, waarbij 4 fasen van ontwikkeling zijn onderkend voor GRC. Daarnaast zijn additionele interviews gehouden en de verkregen inzichten zijn op diverse plaatsen in dit rapport verwerkt. Het gemiddelde ontwikkelingsbeeld ziet als volgt uit:



Het diagram toont dat ondernemingen hoge ambities hebben op GRC-gebied en dat deze steeds de huidige inschaling, die ook niet gering is, overstijgen. De projectgroep wil graag de belangrijkste uitkomsten door middel van dit discussierapport aan de orde stellen, te weten: 1) het huidige niveau van de aanwezige kennis en kunde, 2) het hoge geambieerde ontwikkelingsniveau, 3) de mate van integratie en 4) de prestatiemeting.

Is deze hoge ambitie reëel in het licht van de huidige ontwikkelingen? In samenwerking met de branche- en netwerkorganisaties en grote opdrachtgevers willen de onderzoekers de dialoog openen met toezichthouders en bestuurders van bouwondernemingen en aanverwante organisaties.

Uit aanvullende diepte-interviews met de leiding van bouwondernemingen blijkt dat de bouwsector in de nasleep van de bouwaffaire hard heeft gewerkt aan het verbeteren van het GRC-speelveld. Er zijn aanzienlijke vorderingen gemaakt in de afgelopen jaren, maar desalniettemin zijn er nog de nodige uitdagingen om verbetering te realiseren. Uit het onderzoek blijkt dat er behoefte is aan verdergaande ontwikkelingen op het gebied van interne beheersing en integratie van GRC-functies.

Aanbeveling

De projectgroep heeft een GRC-normenkader voor de bouwsector ontwikkeld. Het normenkader geeft een overzicht van belangrijke aspecten van GRC in de bouw, uitgedrukt in subaspecten met daarbij de kenmerken behorend bij een 4-fasen ontwikkeling. De projectgroep beveelt toezichthouders, bestuurders en management van Nederlandse bouwondernemingen aan het specifiek voor de bouwsector ontwikkelde normenkader, zoals opgenomen in bijlage 3, te implementeren en haar onderneming periodiek hieraan te toetsen. Aan de branche- en netwerkorganisaties vraagt de projectgroep aandacht voor deze aanbeveling.

02 | GRC-speelveld en achtergrond in het kort

Zowel private als publiekrechtelijke organisaties zijn op zoek naar een juist instrumentarium om aan de 'lawine van eisen', een efficiënte en effectieve invulling te geven. Een deel van de mogelijke oplossingen is gelegen in een gebalanceerd raamwerk van GRC. Er bestaat geen eenduidige definitie voor het begrip GRC. Voor het doel van dit discussierapport gebruikt de projectgroep de volgende omschrijving:

GRC is de combinatie van processen en structuren die het bestuur van een organisatie heeft geïmplementeerd om de activiteiten van informatie te voorzien, te sturen, te managen en te monitoren bij het bereiken van haar doelstellingen.

Bouwsector

Op grond van recente ontwikkelingen in de bouwwereld, zoals een sterk veranderende markt met stagnatie van nieuwbouw in de woning- en kantorenmarkt is deze sector geselecteerd om een onderzoek naar de GRC status quo te doen en gelijktijdig de ambitie in beeld te brengen. Het onderzoek is opgesteld door GRC-professionals die vanuit hun dagelijkse praktijk gewend zijn grote ondernemingen tegen het licht te houden. Uitgaande van onder meer Cobouw-informatie, zijn de 15 grootste bouw- en aanverwante ondernemingen geselecteerd en benaderd met het verzoek of zij aan dit onderzoek wilden meewerken. Omdat ook opdrachtgevers baat hebben bij een gezond GRC-speelveld, is tevens een tweetal grote opdrachtgevers, Rijkswaterstaat en Rijksgebouwendienst, om hun medewerking gevraagd.

Dat GRC leeft, blijkt uit het feit dat 10 van de 15 ondernemingen en beide opdrachtgevers hun medewerking toezegden en hun beloftes ook daadwerkelijk gestand deden. Vanzelfsprekend is aan alle betrokkenen volledige anonimiteit toegezegd.

GRC-normenkader

Voorafgaand aan het contact met ondernemingen en opdrachtgevers is de aanpak ontwikkeld. GRC is nog duidelijk een vakgebied in ontwikkeling. Het door de projectgroep gehanteerde GRC-normenkader voor de meting is ontwikkeld op basis van beschikbare literatuur en eigen kennis en ervaring. In discussiebijeenkomsten is het concept van de subassen ontwikkeld om de drie abstracte hoofdbegrippen van GRC hanteerbaar te maken (zie bijlage 3).

De keuze van de te meten aspecten, de subassen van GRC, beoogt niet zo zeer het beste model te zijn als wel een goed uitgangspunt met een overzichtelijke hoeveelheid te meten aspecten. Per subas zijn kenmerken van een 4-tal ontwikkelingsfases gedefinieerd. De projectgroep realiseert zich heel goed, dat het GRC-speelveld aan verandering onderhevig is en staat open voor suggesties bij het eventueel aanpassen van het toekomstige normenkader. Dit geldt eveneens voor mogelijk op te stellen modellen voor andere sectoren in de Nederlandse industrie en handel. Het door ons ontwikkeld model is specifiek ontwikkeld voor de bouwsector. Bij de ontwikkeling van normenkaders in andere sectoren zullen andere specifieke branche aspecten in acht genomen dienen te worden.

Rapportstructuur

In het nu volgende hoofdstuk worden de samenvattende conclusies in de vorm van discussiepunten geresumeerd. Deze punten zullen in een bijeenkomst worden besproken. In hoofdstuk 4 volgt een opsomming van de good practices, zoals die uit het onderzoek blijken. In hoofdstuk 5 worden de gedetailleerde trends uit het onderzoek naar de afzonderlijke GRC-deelgebieden beschreven. Hoofdstuk 6 geeft meer detail informatie over onze aanpak en in hoofdstuk 7 volgt een uitgebreide toelichting op het gehanteerde model voor de GRC-meting aan de hand van het gehanteerde GRC-normenkader.

03 | Discussiepunten

De samenvattende conclusies worden weergegeven als discussiepunten. De projectgroep beoogt met deze punten de dialoog te openen voor het onderwerp GRC bij raden van commissarissen, raden van bestuur en senior management van Nederlandse bouwondernemingen. De aanbeveling is gericht aan dezelfde groep. Verder wordt aandacht gevraagd voor GRC bij branche- en netwerkgroepen zoals Bouwend Nederland, Vernieuwing Bouw en MKB Nederland. De belangrijkste punten betreffen:

Discussiepunt 1

Zijn kennis en kunde over geïntegreerde GRC-toepassingen van voldoende niveau in de bouwsector om adequaat te kunnen inspelen op de zo snel veranderende markten en omstandigheden? Een cruciaal onderdeel van het GRC-speelveld is risicomanagement en dit kent een sterke focus op projectrisico's. Risico's nemen toe doordat aan opdrachtportefeuilles langlopende activiteiten worden toegevoegd zoals onderhoud, beheer, service en de samenwerking in consortia. In toenemende mate wordt gebruik gemaakt van geïntegreerde bouworganisatievormen, waarbij naast uitvoeren ook ontwerpen en andere functies worden vervuld. Op dit gebied is GRC en vooral risicomanagement nog sterk in ontwikkeling en bestaat er nog geen eenduidige en transparante aanpak.

Hebben bouwondernemingen voldoende kennis en kunde van GRC en specifiek enterprise risk management (ERM) om de huidige ontwikkelingen te beheersen?

Discussiepunt 2

De bouwsector laat een hoog ambitieniveau voor de GRC-aspecten zien (zie grafiek op pagina 5). Governance Policy (GP), Bedrijfsethiek (BE), Maatschappelijk Verantwoord Ondernemen (MVO), Risk Framework (RF), Transparantie, Zichtbaarheid & Commitment (TZC), Reputatie (R), Compliance (C), Monitoring & Performance Management (MPM) en Ondersteunende Afdelingen (OA), scoren alle tegen de waarde 4 aan, terwijl de huidige inschaling rond de waarde 3 ligt.

Is de huidige inschaling niet aan de rooskleurige kant en is de ambitie niet te hoog? Welke concrete stappen wil de sector nemen om de ambities te bereiken?

Discussiepunt 3

GRC-functies zijn aanwezig in de bouwsector, maar de geïntegreerde aanpak en samenwerking tussen de verschillende functies kan nog verder worden verbeterd. In de huidige situatie zien we de GRC-functies terug als op zich zelf staande silo's waarbij kennis blijft hangen bij specialisten, waardoor relevante informatie niet doorkomt bij de top van de ondernemingen en zo het risico op verkeerde beslissingen toeneemt. Het streven om heldere en relevante informatie naar de top te krijgen wordt niet ondersteund door periodieke onafhankelijke toetsingen op operaties en risicomanagement, door een onafhankelijk Internal Audit Functie (IAF). Daarnaast kijken opdrachtgevers tegenwoordig naar de functionaliteit van de bouw en niet naar het gespecificeerd product. De toenemende complexiteit van contracten, met verlegging van de risico's naar de opdrachtnemer, vragen om een integrale benadering waarin alle GRC-aspecten worden meegewogen, vooral bij samenwerkingsverbanden van meerdere ondernemingen.

Kan het management de juiste beslissingen nemen over risico's omtrent bijvoorbeeld groeidoelstellingen, voorfinancieringen, aanbestedingsprocedures, netto werkkapitaal, grondposities, afval, integriteit, klokkenluiders en prestatiebeoordelingen bij afwezigheid van een geïntegreerd GRC-speelveld?

Discussiepunt 4

Integriteit en transparantie staan onder voortdurende aandacht van de leiding van bouwondernemingen en er is veel aandacht voor implementatie van gedragscodes en het verankeren van normen en waarden in de genen van de medewerkers. Maatschappelijk verantwoord ondernemen (MVO) speelt hierin een belangrijke rol. Het op structurele wijze toezien op de naleving en meten van de resultaten wordt nog niet consistent toegepast. Vaak is de leiding incident gedreven en redeneert men dat het opvolgen van incidenten voldoende is om implementatie van deze gedragscodes te realiseren. MVO zit nog niet in de genen van de bouwsector.

Is prestatiemeting op gebied van transparantie en integriteit- als onderdeel van MVO - voldoende geïmplementeerd?

04 | Good practices

Een good practice is de term voor algemeen aanvaarde normen en standaarden voor het beheersen van risico's en controls binnen het GRC-speelveld, die bij juiste toepassing, als voldoende beoordeeld en herkenbaar zijn voor GRC-specialisten. Kort gezegd geven good practices aan wat u in de praktijk kunt doen om GRC adequaat te implementeren. Hieronder volgt een opsomming van good practices uit het onderzoek:

Good practice 1 - Aanpassen aan de veranderende markt

De markt is veranderd door toepassing van geïntegreerde contracten. De bouwsector dient de beheersmiddelen daarop aan te passen. Partijen moeten aangeven dat hun product de vereiste functionaliteit heeft. Vroeger werd er veel verrekend via meer- en minderwerk, maar in de nieuwe opzet hanteren opdrachtgevers een systeemgerichte contract controle. Die controle dient open te staan voor het bespreekbaar maken van gerezen problemen en het zoeken naar oplossingen. Kleine partijen kunnen gaan samenwerken in grotere verbanden om als serieuze speler te worden beschouwd. Wel dienen zij hun organisatie en governance aan te passen.

Good practice 2 - Geïntegreerde risicoaanpak

Naast risicobeheersing op projectniveau dienen ondernemingen over een gedifferentieerd risicoprofiel te beschikken dat wordt gesteund door het bestuur en de raad van commissarissen. Het gaat er niet alleen om de kansen en bedreigingen uit hoofde van projecten in kaart brengen, maar ook de geïntegreerde aanpak en cumulatie van risico's op het gebied van financiën, treasury, internationale samenwerkingsverbanden en reputatie.

Good practice 3 - Kennis van techniek én financiën in relatie tot de omgeving

Bij beheersing van projecten zijn kennis van techniek en financiën complementair. Ze dienen onlosmakelijk verbonden te zijn zodat zij de interne beheersing en de balans met de omgeving ten goede komen.

Good practice 4 - Periodieke onafhankelijke toetsing als onderdeel van GRC

Binnen de bouwsector bestaat een sterke oriëntatie op eerstelijns functies. De tweedelijns business controllers en groepsstaven zijn zo lean & mean als mogelijk. Het merendeel van de bouwondernemingen maakt geen gebruik van periodieke onafhankelijke toetsingen op GRC-functies. Juist onafhankelijke toetsingen, zoals bijvoorbeeld door een Internal Audit Afdeling (IAF) als derdelijns functie met een primaire focus op operaties en risicomanagement, dragen bij aan een betere beheersing van de onderneming. Dat leidt tot een versterking van de eerste en tweede lijn en geeft het top management meer zekerheid.

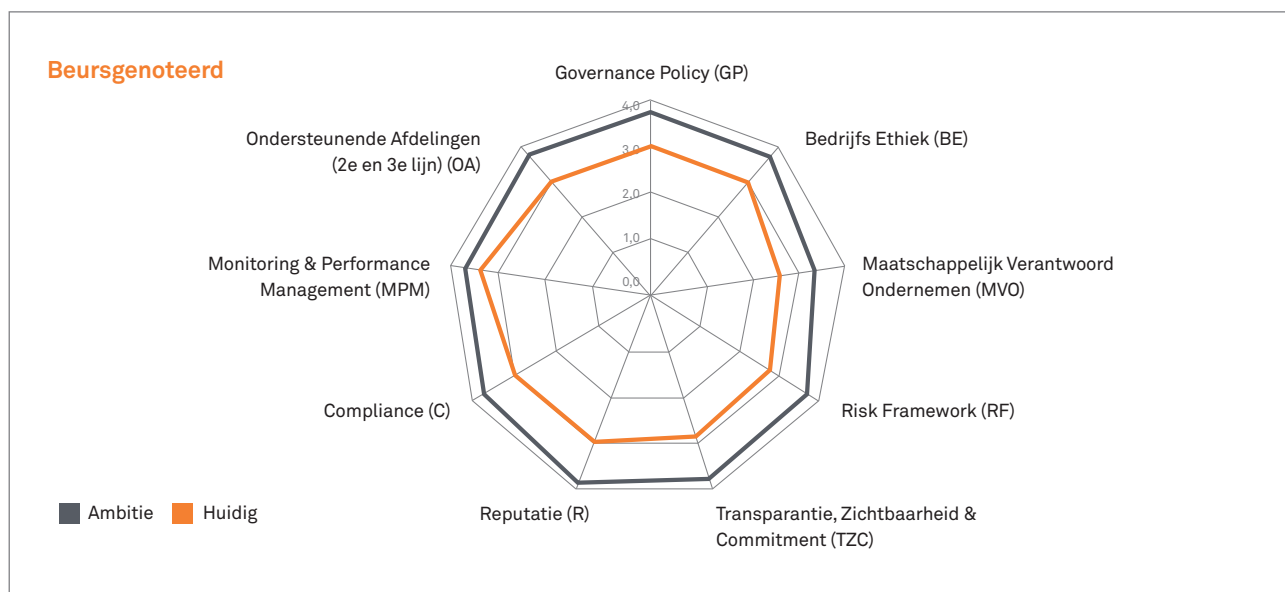
Good practice 5 - Ontwikkelen communicatievisie

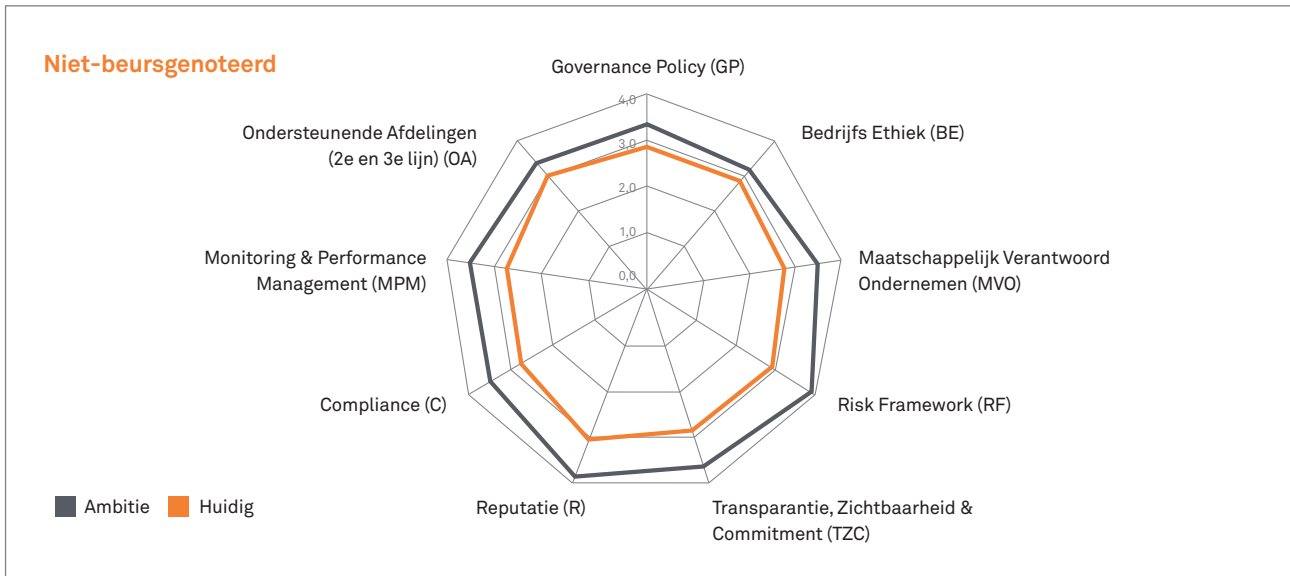
Samenwerken, kennis delen en communicatie zijn in het kader van GRC van groot belang. Om risico's te managen is interne communicatie binnen projecten, tussen deelnemende bouwparticipanten en naar de top van de ondernemingen, van cruciaal belang. De bouwondernemingen dienen meer aandacht te besteden aan communicatie en een visie hierop te ontwikkelen. Hierin dient op gepaste wijze plaats te zijn voor strikte protocollen en sociale media als Facebook, LinkedIn en Twitter, om kennis te delen en risico's zoals bijvoorbeeld faalkosten te beperken.

05 | GRC in de bouw

In dit hoofdstuk wordt per deelgebied van het GRC-speelveld een analyse met toelichting gegeven op de resultaten van het onderzoek. De spindiagrammen zijn tot stand gekomen door de gewogen gemiddelden van de scores (1 t/m 4) van de 10 ingevulde vragenlijsten voor inschaling van de huidige en geambieerde fasen.

Het totale gemiddelde GRC-ontwikkelingsbeeld, uitgesplitst naar beursgenoteerde en niet-beursgenoteerde bouwondernemingen, ziet als volgt uit:





Opvallende verschillen tussen beursgenoteerde en niet-beursgenoteerde ondernemingen zijn in onderstaande analyses verwerkt. De getallen in de grafieken en de onderstaande teksten zijn om trends en verschillen weer te geven. Zij beogen niet een exactheid, daarvoor is het aantal ondernemingen te klein en is de verificatie enkel en alleen door diepte interviews ten enenmale ontoereikend. Hierna volgt een analyse en uitleg van de GRC-hoofd- en subassen.

5.1. Governance

Samenvattende conclusie

De ondernemingen geven aan dat de ambitieniveaus van GP, BE en MVO hoger liggen dan hun inschattingen van de huidige inschaling op deze gebieden. Het ambitieniveau ligt gemiddeld genomen tussen de 3 en 4; de huidige inschaling gemiddeld genomen tussen de 2 en 3. Uit de aanvullende interviews is gebleken dat alle ondernemingen bewust bezig zijn met een ontwikkeling om de governance van de onderneming te versterken. Beursgenoteerde ondernemingen hebben voor GP en BE een wat hoger ambitieniveau dan niet-beursgenoteerde ondernemingen. Ook qua realisatie schalen beursgenoteerde ondernemingen zich op deze twee assen wat hoger dan niet-beursgenoteerde ondernemingen. Op het gebied van MVO is nagenoeg geen verschil te onderkennen.

Conclusies voortvloeiend uit de afzonderlijke subassen

Governance Policy (GP)

- Divisie en concernleiding staan verder af en in de cultuur van bouwondernemingen is het niet overal gebruikelijk open en transparant bottom-up te rapporteren wat er echt aan de hand is. Verschillende ondernemingen zijn bezig met meer top down gerichte trajecten om projectinformatie, met betrekking tot tijd, geld, kwaliteit, informatie en organisatie, risicomanagement en compliance, over de projecten en ondernemingen heen verder en beter te integreren. Tussen beide informatiestromen is echter sprake van een disconnectie. Eén van de mogelijke oorzaken van de disconnectie is het ontbreken van duidelijke strategische doelstellingen en een richting geven aan de organisatie waarbinnen interne beheersing van risico's en controls centraal staan. Onafhankelijke periodieke internal audits kunnen deze informatie 'ophalen' en naar de top brengen. Dit draagt bij aan adequate informatievoorziening aan de leiding van de bouwondernemingen.
- Huidige marktontwikkelingen, de eurocrisis en veranderende risico's vragen om een andere governance benadering met specifieke aandacht voor cultuur en bedrijfsethiek, naleving van policies en aandacht voor maatschappelijk verantwoord ondernemen. De veranderingen gaan heel snel en eigenlijk moet getoetst kunnen worden aan de norm van morgen. De bouwsector zal sneller en adequater moeten inspelen op veranderingen.

- In de besturingsmodellen hebben de lokale werkmaatschappijen primair een eigen verantwoordelijkheid voor risicomanagement en compliance. Aandacht voor governance is nog minder ontwikkeld, zowel op de huidige als de geambieerde inschaling van de onderzochte ondernemingen.
- Het kost relatief veel energie om bij bouwondernemingen aandacht voor het onderwerp governance (cultuur, bedrijfs-ethiek, policies, procedures, MVO etc.) te kweken. De huidige cultuur is meer hands-on op de projecten gericht en governance wordt als extra ballast ervaren. Medewerkers worden (nagenoeg) niet betrokken bij de bepaling van de doelstellingen van de ondernemingen en op dit gebied kan nog veel worden gewonnen.
- Tegenwoordig komen geïntegreerde bouwcontracten op ruime schaal voor. Bij grote ondernemingen vinden veranderingen plaats door overgang van rationalisatie en automatisering grond-, water- en wegenbouw (RAW) bestekken naar Design, Build, Finance, Maintain & Operate contracten (DBFMO). Deze veranderingen vragen om een andere governance. Kennis verdwijnt bij opdrachtgevers en de positie van de aannemers wordt veel sterker en machtiger. Om de reputatie te waarborgen dient de governance hierop aangepast te worden.

Business Ethiek (BE)

- De onderzochte ondernemingen geven aan dat ambitieniveaus voor BE hoger liggen dan hun inschattingen van de huidige inschaling op dit gebied. Uit de aanvullende interviews is gebleken dat alle ondernemingen bewust bezig zijn met een ontwikkeling om de BE van de onderneming te versterken.
- Beursgenoteerde ondernemingen hebben voor BE een wat hoger ambitieniveau dan niet-beursgenoteerde ondernemingen. Ook qua huidig niveau schalen beursgenoteerde ondernemingen zich op deze as wat hoger in dan niet-beursgenoteerde ondernemingen.

Maatschappelijk Verantwoord Ondernemen (MVO)

- De onderzochte ondernemingen geven aan dat de MVO ambitieniveaus hoger liggen dan hun inschattingen van de huidige inschaling op deze gebieden. Uit de aanvullende interviews is gebleken dat alle ondernemingen bewust bezig zijn met een ontwikkeling om MVO te versterken.

5.2. Risicomanagement

Samenvattende conclusie

Risicomanagement speelt al jaren een belangrijke rol bij beheersing bij projecten in de bouwwereld. Het systematisch vastleggen van deze risico's in assessments op grond van een risicomanagementraamwerk en het consolideren tot een organisatiebrede risicoassessment begint geleidelijk aan vorm te krijgen. De wens om te kunnen beschikken over een organisatiebreed risicodashboard leeft duidelijk op topmanagementniveau. Een organisatiebreed risicoassessment is zelfs onontbeerlijk in situaties waarin sprake is van:

- Doorwerken van individuele projectrisico's op risico's in andere projecten;
- Sterk fluctuerende grondstofprijzen;
- Toenemende ondernemingsdiversificatie door het offrenen van geïntegreerde contacten;
- Samenwerken met andere ondernemingen in consortia al of niet in samenhang met PPS.

Uit de analyse van de Plan-Do-Check-&-Act-controlloop (PDCA) van het risicomanagementraamwerk blijkt dat de laatste schakels waarin bijvoorbeeld de follow-up van de acties om een risico te mitigeren, minder ver ontwikkeld zijn dan de voorafgaande schakels. Externe risicofactoren worden in kaart gebracht, maar het beeld is wel dat het nog stelselmatiger en daardoor vollediger zou kunnen. Het belang van het risicomanagement raamwerk blijkt uit de sterke ambitie van alle ondernemingen, beursgenoteerd en niet-beursgenoteerd om het risicomanagement op een hoger niveau te brengen.

Conclusies voortvloeiend uit de afzonderlijke subassen

Risk Framework (RF)

- Alle ondernemingen beschikken over een risicobeleid, maar wel in verschillende stadia van ontwikkeling. Het valt op

dat het risicomanagement op individuele projecten en op divisioneel niveau beter ontwikkeld is dan op overall corporate niveau.

- De mate van implementatie en communicatie van het risicoraamwerk in een organisatie hangt in hoge mate samen met het niveau waarop het risico raamwerk is ontwikkeld. Te veel sturing vanuit de top werkt averechts op de werkmachtschappijen, die heel goed weten wat hun risico's zijn. Te veel administratieve lastendruk bij de werkmachtschappijen belemmert de echte risicoinformatie naar boven.
- De risico's inherent aan de projecten worden diepgaand geïnventariseerd, besproken en gemonitord en zo nodig vinden adequate acties plaats. De PDCA-controlloop voor de overall geconsolideerde risico's bevindt zich nog duidelijk op een lager niveau van ontwikkeling.

Transparantie, Zichtbaarheid & Commitment (TZC)

- Bij de onderzochte ondernemingen is het ownership voor risicomanagement duidelijk ingevuld en is hiervoor aandacht van het bestuur. Als er al een aparte functie voor in het leven is geroepen, dan is die veelal kleinschalig, zeker bij projecten geldt dat het projectmanagement geacht wordt zelf de risicoassessment op te stellen.
- Wel blijkt dat bij beursgenoteerde ondernemingen het ownership hoger in de organisatie ligt dan bij niet-beursgenoteerde ondernemingen. Dan blijkt ook dat het risicomanagement niet enkel en alleen een kunstje voor projectbeheersing is.
- Risicorapportage is intern gericht. In een enkel geval vond er in een recent jaarverslag een uitgebreide rapportage plaats. De verwachting is overigens wel dat deze openheid zich verder gaat ontwikkelen.
- Zeker bij projecten vinden desgewenst de nodige acties plaats teneinde de consequenties van een risico zoveel mogelijk te mitigeren.

Reputatie (R)

- Reputatie is een onderwerp dat hoog op de agenda staat bij bestuur en raad van commissarissen. Het valt op dat de aandacht voor dit onderwerp bij niet-beursgenoteerde ondernemingen iets sterker is dan bij beursgenoteerde ondernemingen.
- Gezien het belang dat aan een goede reputatie wordt gehecht, is er over het algemeen behoorlijk zicht op de risico's.
- In samenhang met de voorafgaande conclusies blijkt dat er belang wordt gehecht aan reputatiemanagement en dat er early warning systems zijn. De mate van ontwikkeling varieert sterk.
- Voor een bouworganisatie is het van groot belang om bij langdurige projecten de risico's voortvloeiend uit (sterk) fluctuerende grondstofprijzen vroegtijdig te onderkennen en de daarmee samenhangende risico's uit de eventuele hedgingactiviteiten. Een proactieve houding naar de opdrachtgevers, waarbij positieve en negatieve effecten worden verrekend, dragen bij aan de reputatie van bouwondernemingen.
- Veiligheidsrisicoassessments zijn onontbeerlijk in de bouwwereld.
- Zowel qua aantal als qua impact kunnen risico's fors stijgen bij de toename van de one-stop-benadering waarbij een klant in één keer van alle markten en producten wordt voorzien in wensen die voortvloeien uit een overall project. Een dergelijke geïntegreerde aanpak (bijvoorbeeld ondernemingsdiversificatie waarbij ook bouwvreemde activiteiten als financiering, catering en full service contracten worden meegenomen) leidt veelal tot een cumulatie van risico's.

5.3. Compliance

Samenvattende conclusie

De scores van zowel beursgenoteerde als niet-beursgenoteerde bouwondernemingen zitten wat betreft C, MPM en OA dicht bij het ambitie niveau welke zij nastreven. De bouwaffaire is een sterke impuls geweest om gedragsregels en bevoegdheden te formaliseren en het voldoen aan deze regels te bewaken. Bij de meeste bouwondernemingen wordt compliance primair vanuit een juridische invalshoek benaderd, waarbij er steeds meer aandacht is voor de gedragsfactor van de medewerkers en hoe compliance dit organiseert.

De meeste bouwondernemingen zijn sterk decentraal georganiseerd met een beperkt aantal stafafdelingen. Op top management niveau is men tevreden over het functioneren en de onderlinge samenwerking van deze stafafdelingen.

De financiële functie vervult veelal de monitorende en toetsende rol om naleving van (administratieve) procedures binnen de organisatie periodiek te controleren. In de bouwsector bestaat een verkeerd beeld van de rol van een internal auditor, die juist gericht is op het behalen van de strategische doelstellingen met bijbehorende risico's en controls. Slechts enkele van de onderzochte bouwondernemingen heeft een aparte interne audit functie (IAF). Als reden voor de afwezigheid van deze functie wordt aangegeven dat deze niet zou passen in de ondernemingscultuur, de omvang van de organisatie of dat geen toegevoegde waarde wordt verwacht van de IAF.

Conclusies voortvloeiend uit de afzonderlijke subassen

Compliance (C)

- De onderzochte bouwondernemingen geven aan dat hun ambitie voor het beleggen van verantwoordelijkheden voor compliance binnen de organisatie achterblijft op de realisatie. Bijna de helft van de ondernemingen moet nog de verantwoordelijkheden voor compliance beleggen. Bij deze ondernemingen zijn medewerkers niet verantwoordelijk voor compliant zijn en wordt dit niet goed gemeten. Eindverantwoordelijkheid moet door medewerkers worden gedragen, waarbij een afdeling compliance het proces faciliteert.
- Bij de meeste bouwondernemingen wordt compliance in eerste instantie vanuit een juridische invalshoek benaderd. Het aanstellen van vertrouwenspersonen en het vaststellen en communiceren van ethische gedragsregels heeft hierbij de afgelopen jaren de primaire aandacht gehad. Met behulp van onder meer promotietours, rollenspellen en ethische vraagstukken zijn medewerkers bekend gemaakt met de gedragsregels.
- Een periodieke toetsing van de bekendheid met gedragsregels blijft meestal achterwege en vormt geen onderdeel van het interne beheersingsmechanisme. Bij een aantal (beursgenoteerde) bouwondernemingen zijn hiervoor al wel aparte compliance officers benoemd. De kleinere (niet-beursgenoteerde) bouwondernemingen zeggen bij voorkeur te steunen op hun platte organisatiestructuur, de open communicatie en het netwerk van vertrouwenspersonen.
- Slechts de helft van de onderzochte bouwondernemingen voert periodieke toetsingen uit op de naleving van compliance gerelateerde regelgeving. De overige ondernemingen zeggen vooral te steunen op een sterke financiële functie als waarborg dat ook eventuele compliance gerelateerde issues tijdig worden gedetecteerd en gerapporteerd.

Monitoring & Performance Management (MPM)

- De onderzochte bouwondernemingen geven aan dat de huidige niveau van MPM dicht bij het ambitieniveau ligt. De niet-beursgenoteerde bouwondernemingen scoren lager wat betreft MPM, terwijl de ambitie vergelijkbaar is met die van beursgenoteerde bouwondernemingen.
- Het financiële rendement van bouwers is generiek vrij laag en reductie van faalkosten wordt door vrijwel alle bouwers genoemd als een primair doel om de financiële performance te verbeteren. Door ondermeer standaardisering van werkprocessen, collegiale toetsingen op projectniveau en ondernemingsreviews wordt de performance van ondernemingsonderdelen vergeleken en gemonitord.
- Bij drie van de onderzochte bouwondernemingen is hun mission statement nog niet eenduidig vastgelegd en gecommuniceerd. Uit de interviews blijkt verder dat er veel algemeen geformuleerde mission statement worden gehanteerd.
- Het monitoren van de werkelijke prestaties ten opzichte van meer specifiek gedefinieerde doelstellingen wordt nog niet regelmatig uitgevoerd. Op corporate niveau ontbreekt vaak een dashboard voor MPM en er is beperkte aandacht voor het definiëren en monitoren van key performance indicators (KPIs).

Ondersteunende Afdelingen (OA)

- Bouwondernemingen geven aan dat zij beschikken over een coherent raamwerk van ondersteunende afdelingen/functies op concern niveau. Deze afdelingen zijn professioneel en werken nauw samen. De concernstaven zijn veelal gering en qua omvang concentreren zij zich met name op juridische en financiële aangelegenheden.
- Slechts enkele van de bouwondernemingen hebben een aparte internal audit functie (IAF). De meeste geïnterviewden geven hierbij aan dat een aparte IAF niet zou passen bij de cultuur en omvang van de eigen onderneming. Een aparte IAF wordt veelal gezien als toetsing op naleving van belasting- en boekhoudregels. Hoewel de Nederlandse corporate governance code het hebben van een IAF voorschrijft geven verschillende beursgenoteerde ondernemingen er de

voorkeur aan deze toetsende rol uit te laten voeren door de externe accountant, vaak in samenwerking met medewerkers van centrale financiële afdeling en controllers van de werkmaatschappijen.

- Verschillende bouwondernemingen hanteren vooral het instrument van collegiale toetsingen (peer review) waarbij in het geval van grote projecten een deskundig en ervaren team van een andere werkmaatschappij een kritische doorlichting uitvoert en hierover verslag doet aan het bestuur.
- Door toenemende standaardisering van IT-systemen, processen en uniformering van werkwijzen is een tendens te herkennen tot centralisering van staffuncties. Echter vanwege kostenopslagen voor overhead, welke bouwondernemingen hanteren in calculaties, is er beperkte financiële ruimte om te investeren in de eigen organisatie.
- Het ontbreken van een IAF wordt door de meeste ondernemingen gecompenseerd door periodieke overleggen met lokale directies waarbij kritisch de betreffende organisatie en projecten inhoudelijk worden doorgenomen. Op deze wijze zeggen de besturen voldoende grip te hebben op de eigen organisatie.

06 | Aanleiding en werkwijze onderzoek

6.1. Aanleiding

Enkele jaren geleden stond de bouwsector in het middelpunt van de belangstelling door onregelmatigheden bij de aanbesteding en gunning van overheidsprojecten. De bouwaffaire kwam tot een climax en werd in 2002 onderzocht in een parlementaire enquête. 244 Nederlandse bouwondernemingen maakten zich schuldig aan fraude. Op 11 februari 2005 kwam de bouwwereld met de regering een schadevergoeding overeen van 70 miljoen euro. Recentelijk werd in de kranten melding gemaakt van het faillissement van de Koop Groep, een voormalige grote speler in de bouwsector. De kranten waarschuwen voor moeilijkere tijden met een stijging van failliete bouwondernemingen met maar liefst 13% tot 1.126 in totaal in 2011. “De kredietcrisis werkt als een accelerator en allerlei bouwondernemingen, groot en klein, moeten eraan geloven”.

Voorvallen als hierboven roepen de vraag op: “Hoe goed zijn bouwondernemingen nu eigenlijk in control en gewapend tegen risico’s?”, of meer gedetailleerd: “Hoe is GRC ingebed in de interne beheersingsorganisatie van bouwland Nederland?”. In 2010 publiceerde de Nederlandse Beroepsorganisatie van Accountants (NBA) en het Instituut van Internal Auditors Nederland (IIA) de publicatie “De internal auditor als spin in het GRC-web”. Het rapport kent een prominente rol toe aan de Internal Audit Functie (IAF) op het gebied van GRC, enerzijds als onderdeel van de governance organisatie en anderzijds als de eigen toetsende verantwoordelijkheid op de organisatie. Een aantal leden van de projectgroep borduurde voort op het rapport en ontwierp een 4-fasen ontwikkelingsmodel voor de belangrijkste spelers in het GRC-speelveld in de bouwsector.

Gezien bovenstaande voorvallen, de decentrale opbouw van de bouworganisaties en de afwezigheid van één of meer cruciale spelers in het GRC-speelveld, volgt hier de centrale onderzoeksvraag voor het onderliggende discussierapport:

Hoe scoren bouwondernemingen als het gaat om de mate van ontwikkeling op GRC-gebied en hebben zij een ambitie zich te verbeteren?

De projectgroep van dit GRC-project geeft haar antwoord op deze vraag in de voorgaande hoofdstukken, waarin tevens samenvattende conclusies en aanbevelingen zijn geformuleerd voor de branche- en netwerkorganisaties, de raden van commissarissen, de raden van bestuur en alle andere GRC-geïnteresseerden. In hoofdstuk 7 wordt tekst en uitleg bij het voor de bouwsector ontworpen GRC-ontwikkel model gegeven.

6.2. Werkwijze onderzoek

Als vervolg op het artikel in 'Accountant' (maart 2011) heeft de projectgroep een normenkader uitgewerkt voor een eerste GRC-meting in de bouwsector. Het normenkader kent 4 fasen van ontwikkeling en is nader toegelicht in hoofdstuk 7 van dit rapport.

Het onderliggend rapport is het resultaat van een onderzoek naar de 15 grootste bouwondernemingen in Nederland. Naast een literatuuronderzoek op basis van publiekelijk toegankelijke informatie, zijn de bouwondernemingen benaderd en gevraagd een vragenlijst in te vullen en aan te geven in welke fase zij zich bevinden en op welk niveau hun ambitie ligt. De bouwondernemingen zijn uitgenodigd deze vragenlijst tijdens een interview toe te lichten. 10 bouwondernemingen hebben meegewerkt aan het onderzoek.

Dit discussierapport is geschreven in opdracht van de Ledengroep Intern en Overheidsaccountants (LIO) van de NBA. Het onderzoek omvat een analyse van een anonieme GRC-ontwikkelingsbenchmark van verschillende bouwondernemingen in Nederland. Beoogt wordt de verkregen kennis te delen met leden van de Raden van Commissarissen, leden van de Raden van Bestuur, directies en management en alle andere GRC-geïnteresseerden in de bouwsector, als ook aanverwante organisaties, branche- en netwerkorganisaties en opdrachtgevers als Rijkswaterstaat en de Rijksgebouwendienst. Tenslotte kan het ontwikkelde GRC-model de basis vormen voor een GRC-ontwikkelmodel in andere sectoren in Nederland en kunnen tevens de good practices van belang zijn voor de andere sectoren om hiermee hun voordeel mee te behalen.

07 | GRC-ontwikkeling en uitleg model

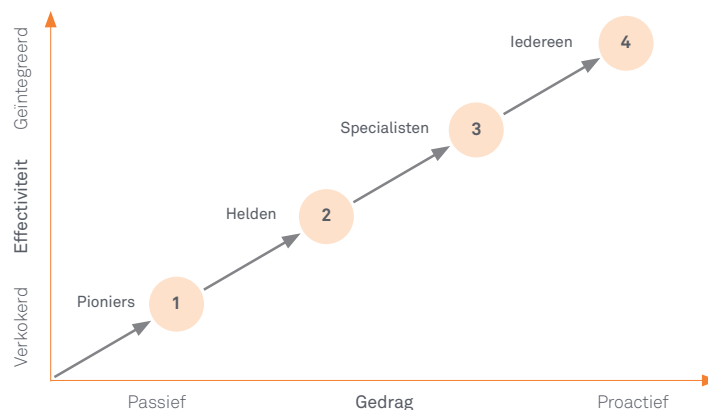
Het bouwen aan een GRC-raamwerk is een complexe en intensieve aangelegenheid. Een gedegen GRC-raamwerk vergt inbreng van alle gelederen van een organisatie, is multidisciplinair van karakter en is per definitie klantspecifiek. Het is dan ook niet ongewoon om een plan van aanpak te maken waarin doelstellingen over de te bereiken GRC-niveaus en onderdelen, en de weg erheen (met mijlpalen) zijn opgenomen. Normaliter doorloopt een GRC-ontwikkelingsproces een aantal fasen, net als een bouwproject.

De projectgroep heeft voor de Nederlandse situatie een algemeen groeimodel ontwikkeld zoals gepresenteerd in 'Accountant' van maart 2011. Het groeimodel kent vier fasen:

1. Verkokerd en inconsistent;
2. Georganiseerd en reactief;
3. Proactief en gemanaged;
4. Geïntegreerd en geworteld.

De fasen van het groeimodel geven de ontwikkeling weer van 'niets tot alles' in het GRC-speelveld. Pioniers en helden starten met bouwen aan de grondvesten van de GRC-organisatie, waarna specialisten en daarna alle medewerkers in de organisatie deze ontwikkelingen voorzetten tot een zeer geavanceerd en professionele organisatie waarin sprake is van een zeer hoog beheersingsniveau.

GRC-ontwikkelingsmodel



Met bovenstaand groeimodel als uitgangspunt heeft de projectgroep een specifiek GRC-ontwikkelingsmodel met bijbehorend normenkader heeft voor de bouwsector ontworpen. Het normenkader voor de 3 deelgebieden: Governance, Risicomanagement en Compliance kennen per deelgebied 3 subassen.

Aan elk van deze 3 subassen is een 4-fasenindeling gekoppeld. Per fase zijn kenmerken onderkend waaraan in een bepaalde fase moet worden voldaan, alvorens naar de volgende fase kan worden gegroeid. Het gedetailleerde normenkader is in bijlage 3 opgenomen ter documentatie. Uitgaande van het normenkader is een vragenlijst gemaakt waarin exact dezelfde fasen en subassen zijn onderkend, echter met 2 in te vullen niveaus, te weten de huidige situatie en de geambieerde situatie voor een specifieke onderneming.

De bepaling van de subassen is tot stand gekomen door een combinatie van literatuuronderzoek en discussie in de projectgroep. Op basis van de kennisgenomen literatuur en vergelijkbare ontwikkelmodellen is een groslijst gemaakt met mogelijke onderwerpen op de drie deelgebieden Governance, Risicomanagement en Compliance. Om de te bevragen onderwerpen te limiteren tot een lijst met zeer hanteerbare begrippen zijn alle onderwerpen samengevoegd tot een totaal van 27 vragen. Steeds 3 vragen per subas in de logische volgorde van de Plan-Do-Check-&-Act-controlloop (PDAC).

Bijlage 1

Geraadpleegde modellen, artikelen, onderzoeken en links naar websites

Literatuur - modellen

- Red Book 2.1, GRC-Capability Model, Open Compliance & Ethics Group (OCEG), 2012
- Internal Control - Integrated framework, draft for public exposure, Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2011
- Internal Audit Capability Model for the Public Sector, IIA Foundation, 2009
- Nederlandse Corporate Governance Code, Monitoring Commissie Corporate Governance Code, 2008
- Internal Control - Integrated framework, Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2004

Artikelen

- Boon v.d. V., 'Wegenbouwers kochten structureel om', FD 06.01.2011
- Boon v.d. V. / Marel v.d. G., 'Vastgoedzaak koste FIOD liefst 270.000 manuren', FD 03.03.2011
- Broekhuizen K. / Verbraeken H., 'Bouw zakt nog verder weg', FD 18.01.2012
- Croonenberg S. / Geest v.d. E. / Schoevaart M., 'Meetlat voor beheersing', Accountant, maart 2011
- Emanuels J.A. / Munnik de W.G., 'Enterprise Risico Management: een risicobeheersingssysteem voor organisaties', Maandblad voor Accountancy en Ondernemingseconomie, 2006
- Droogsma J., 'Risicomanagementsystemen in de praktijk', Maandblad voor Accountancy en Ondernemingseconomie, 2009
- Groot G. / Winkel R., 'Een frisse wind door het old boy's network', FD 05.11.2011
- Rijendam v. W., 'Miljoenenclaim Koop-top', FD 20.01.2012
- Scheffe J. / Prinsenbergh M. / Manschot J., 'Risicomanagement of crisismanagement?', Bouw + Uitvoering, nummer 3, 2010
- Strikwerda J., 'In-control: zoals geldend in de ondernemingskunde, economie en de cybernetica', November 2011
- Verbraeken H., 'Minister Spies gaat bouwcrisis te lijf met team van experts', FD 19.01.2012

Onderzoeken

- Onderzoeksrapport 'Kansen op weg naar herstel', Pieter van der Zwet, KPMG februari 2012
- Onderzoeksrapport 'Derde rapport over de naleving van de Nederlandse Corporate Governance Code', Monitoring Commissie Corporate Governance, december 2011
- Onderzoeksrapport 'In control & disclosure, through the eyes of the internal auditor', Kee M. / Nieuwlands H. / Danescu D., IIA Nederland, november 2011
- Onderzoeksrapport 'Cobouw 50', oktober 2011
- Publieke management Letter commercieel vastgoed 'Zeg waar het op staat', NBA juni 2011
- Onderzoeksrapport 'De financiële functie in ontwikkeling', Zwet v.d. P. en Waa v.d. F., KPMG, maart 2011
- Transparantiebenchmark 2010 – De Kristal 2010 – Min. v. economische zaken, Landbouw en innovatie i.s.m. NBA, februari 2011
- Onderzoeksrapport 'Governance, risk and compliance: a survey', Marks N. SAP-OCEG fellow, januari 2011
- Onderzoeksrapport 'Het Risicomanagement van Institutionele Vastgoedbeleggers', IVBN 2011
- Onderzoeksrapport 'Cobouw 50', oktober 2010
- Discussierapport 'De internal auditor als spin in het GRC-web', NIVRA en IIA Nederland, september 2010
- Onderzoeksrapport 'Integriteit en Transparantie in de Bouwsector, 1-meting' in opdracht van Vernieuwing Bouw, juli 2010
- Onderzoeksrapport 'Risicomanagement in Nederland', NIVRA-Nyenrode i.s.m. RuG en PWC, 2009
- Onderzoeksrapport 'Beheersing van Frauderisico's in de Institutionele Vastgoedsector', IVBN 2008

Websites

<http://www.bouwendnederland.nl>
<http://www.cobouw.nl>
<http://www.coso.org>
<http://www.monitoringcommissie.nl>
<http://www.oceg.org>
<http://www.rws.nl>
<http://www.rgd.nl>
<http://www.regieraadbouw.nl>
<http://www.sbib.nl>
<http://www.theiia.org>
<http://www.vernieuwingbouw.nl>
<http://nl.wikipedia.org/wiki/Bouwfraude>

Bijlage 2

Afkortingenlijst

| | | |
|-------|---|---|
| AC | - | Audit Commissie |
| BE | - | Bedrijfsethiek |
| DBFMO | - | Design, Build, Finance, Maintain & Operate |
| C | - | Compliance |
| IA | - | Internal Audit |
| IAF | - | Internal Audit Functie |
| GP | - | Governance Policy |
| GRC | - | Governance, Risicomanagement & Compliance |
| KAM | - | Kwaliteit, Arbeid en Milieu |
| KPI | - | Key Performance Indicator |
| MPM | - | Monitoring & Performance Management |
| MVO | - | Maatschappelijk Verantwoord Ondernemen |
| NBA | - | Nederlandse Beroepsorganisatie van Accountants |
| OA | - | Ondersteunende Afdelingen |
| PDCA | - | Plan-Do-Check-&-Act-controlloop |
| PPS | - | Publieke en Private Samenwerking |
| R | - | Reputatie |
| RAW | - | Rationalisatie en automatisering grond-, water- en wegebouw |
| RF | - | Risico Framework |
| RvB | - | Raad van Bestuur |
| RvC | - | Raad van Commissarissen |
| TGKIO | - | Tijd, Geld, Kwaliteit, Informatie en Organisatie |
| TZC | - | Transparantie, Zichtbaarheid en Commitment |

Bijlage 3

GRC-normenkader voor de bouwsector

1 Governance

Governance staat equivalent aan deugdelijk ondernemingsbestuur en behelst de daarin verankerde processen met betrekking tot het besturen, beheersen, verantwoording afleggen en toezichhouden, met het doel de belangrijkste belanghebbenden een goed en transparant beeld van de onderneming te verschaffen en de continuïteit van de onderneming te waarborgen.

| Subas | Fase 1 | Fase 2 |
|--|---|---|
| Governance Policy (GP) | <ul style="list-style-type: none"> • Geen eenduidige en vastomlijnde governance policy; • Geen door wet- en regelgeving afgedwongen governance model aanwezig zoals de Nederlandse Corporate Governance Code; • Governance issues worden ad hoc en incidenteel afgewikkeld. | <ul style="list-style-type: none"> • Governance policy neemt concrete vormen aan; • Governance policy ingesteld o.b.v. algemeen aanvaarde normen zoals de Nederlandse Corporate Governance Code; • De lijn wordt van 'boven af' in het governance proces betrokken; • Governance management reactief n.a.v. incidenten. |
| Bedrijfs Ethiek (BE) | <ul style="list-style-type: none"> • Geen eenduidige en vastomlijnde ethische ondernemingscode; • Geen integriteitworkshops; • Geen klokkenluidersregeling; • Reactieve afhandeling van ethische incidenten. | <ul style="list-style-type: none"> • Ethische visie is door RvB verankerd in cultuur en omgangsnormen; • De 'Tone at the top' is duidelijk; • Lijnmanagement en medewerkers zijn zich bewust van het belang van BE; • Workshops en voorlichting; • Klokkenluidersregeling op papier; • Reactieve afhandeling van ethische incidenten. |
| Maatschappelijk Verantwoord Ondernemen (MVO) | <ul style="list-style-type: none"> • Nog geen gestructureerde corporate visie t.a.v. MVO aanwezig; • Activiteiten op het gebied van MVO zijn verkokerd en inconsistent. Bijvoorbeeld op sommige locaties wordt afval gescheiden en op andere papiergebruik verminderd. Ook wordt lokaal aan milieueisen voldaan, maar er is geen centrale aansturing. | <ul style="list-style-type: none"> • MVO-visie krijgt vorm en is uitgewerkt in een policy met voor de onderneming relevante punten; • Visie wordt uitgedragen vanuit de top naar de BU's, maar de kennis en de kunde zit vooral bij gespecialiseerde afdelingen die MVO-processen managen. |

| | Fase 3 | Fase 4 |
|--|---|---|
| | <ul style="list-style-type: none"> • Volwaardig governance model qua opzet en werking d.m.v. training, workshops en voorlichting voor alle medewerkers; • Werking in de lijn wordt gemeten d.m.v. interviews over kennis en toepassing; • Governance wordt preventief en proactief gemanaged. | <ul style="list-style-type: none"> • Geavanceerde governance policy is verankerd in de gehele organisatie; • De lijn borgt en toetst zelf de governance; • Geïntegreerde rapportages met incidenten en uitzonderingen; • Integratie van governance KPI's in de planning & control cyclus. |
| | <ul style="list-style-type: none"> • 'Tone at the top' en ethische visie i.o.m. feitelijk optreden; • Lijnmanagement en medewerkers zijn doordrongen van het belang van BE; • BE vormt criterium in beoordeling medewerkers; • Integriteitstrainingen; • Transparante afwikkeling van klokkenluidersmeldingen (anonimiteit gewaarborgd). | <ul style="list-style-type: none"> • Ethiek is volledig geïntegreerd in alle ondernemingsprocessen (top down en bottom-up): zit in het DNA van elke werknemer en er wordt naar gehandeld; • Meting van de KPI's van BE d.m.v. continue monitoring en rapportage; • Lering is getrokken uit klokkengeluid d.m.v. (mitigerende) controls en maatregelen; • Continu en geworteld proces ter borging van openheid, helderheid en transparantie. |
| | <ul style="list-style-type: none"> • MVO-visie wordt gedragen door top en middenkader en implementatie van voor de onderneming relevante punten is in alle processen opgenomen; • GRI- en OESO-richtlijnen en RJ400, Accountability Standards, Global Compact van de VN, etc. vormen de basis van MVO-rapportages. | <ul style="list-style-type: none"> • MVO denken en doen is geworteld in de lijn en DNA van de werknemers; • Sustainability index van NYSE en/of de Transparantie benchmark (min. EZ) zijn externe drivers; • MVO-processen geïntegreerd en verankerd met continue control; • Continue MVO-rapportage aan stakeholders via het web. |

2 Risicomanagement

Risicomanagement is een iteratief proces waarin bewust wordt gekozen voor het al dan niet implementeren van beheersingsmaatregelen naar aanleiding van ingeschatte risico's. Risico's zijn ontwikkelingen en gebeurtenissen in de interne en externe omgeving van organisaties die de realisatie van de doelstellingen van de organisatie kunnen bedreigen. Het doel van risicomanagement is op een zo effectief en efficiënt mogelijke wijze te komen tot het realiseren van de doelstellingen van de organisatie. Indien de risico's te groot zijn, dan worden zij verzekerd of, indien de beheersing of de verzekering te duur is, dan worden de activiteiten die aan de doelstelling ten grondslag liggen, beëindigd of kunnen zij worden overgedragen aan andere partijen, waarvoor deze risico's kleiner zijn.

| Subas | Fase 1 | Fase 2 |
|---|--|---|
| Risico Framework (RF) | <ul style="list-style-type: none"> • Geen policy (kennis bij pioniers); • Ad hoc afwikkeling van incidenten; • Geen anticiperende strategische blik op risico's; | <ul style="list-style-type: none"> • Policy in basis vorm aanwezig; • Incidenten worden gedeeld; • Risico bestrijding is vaak nog 'damage control'; • Strategie en processen worden gekoppeld. |
| Transparantie, Zichtbaarheid & Commitment (TZC) | <ul style="list-style-type: none"> • Risico management van pioniers, geen helder proces en rapportage; • Vaste set risico's en ad hoc evaluatie tot bestaande maatregelen. | <ul style="list-style-type: none"> • Aandacht groeit maar zit bij corporate afdelingen; • Policies, rapportages, etc. zijn alleen voor corporate begrijpbaar; • Risico bestrijding is vaak nog 'damage control'. |
| Reputatie (R) | <ul style="list-style-type: none"> • Geen aandacht voor reputatie, alleen ad hoc; • Onderwerp staat niet op de agenda van RvB/RvC en waardoor geen strategische blik op samenhang van risico's; • Weinig ervaring met reputatie risico. | <ul style="list-style-type: none"> • Jaarlijks vaste set risico's; • Samenhang risico's wordt wel reactief besproken, maar geen vooruitziende blik; • Monitoring media reactief en geen consistente benadering. |

| | Fase 3 | Fase 4 |
|--|--|--|
| | <ul style="list-style-type: none"> • Policy volwassen, proactief en begrippenkader; • Periodieke rapportage met mitigerende maatregelen en aandacht voor kansen; • 'Good practices' worden gedeeld. | <ul style="list-style-type: none"> • Policy is geïntegreerd • Elk proces, afdeling en functie brengt risico's (+/-) in kaart en mitigeert gevolgen; • Geïntegreerde rapportage incl. incidenten/kansen. |
| | <ul style="list-style-type: none"> • De betrokkenheid van de lijn stijgt; • Transparantie en zichtbaarheid van het proces; • Periodieke rapportage met kansen en focus top 10 risico's met mitigerende maatregelen. | <ul style="list-style-type: none"> • Betrokkenheid, transparantie en zichtbaarheid alom; • Volledige betrokkenheid; • Ruime ervaring; • Iedereen spreekt dezelfde taal (gedefinieerd). |
| | <ul style="list-style-type: none"> • Focus op top 10 reputatierisico's; • Monitoring van de verschillende media wordt een gemanaged proces. | <ul style="list-style-type: none"> • Geïntegreerd reputatierisico management en benutten van opportuniteiten om de markt te bespelen; • Geïntegreerde rapportage incl. incidenten en uitzonderingen; • Volwaardige reputatieparagraaf; • Optimale monitoring en beïnvloeding verschillende (social) media. |

3 Compliance

Compliance is het begrip waarmee wordt aangeduid dat een organisatie werkt in overeenstemming met vigerende wet- en regelgeving. De compliance functie in een organisatie staat het bestuur bij in haar taak en verantwoordelijkheid om de organisatie in controle te houden in overeenstemming met die wet- en regelgeving. In controle houden wordt dan gezien als het samenspel van instellen, implementeren en monitoren van beheersingsmaatregelen.

| Subas | Fase 1 | Fase 2 |
|--|--|---|
| Compliance (C) | <ul style="list-style-type: none"> • Per operationeel en financieel deelgebied zijn er policies; • Pre-SOx-fase; • Controls en compliance zijn gedreven vanuit juridische zaken, met nadruk op het documenteren. | <ul style="list-style-type: none"> • Steeds meer relevante policies; • Periodieke toetsing van controls (als aparte activiteit) voor operationele en financiële processen; • Compliance wordt onderdeel van normale controls; • Afzonderlijke compliance functionarissen zijn nog wel in de lijn werkzaam. |
| Monitoring & Performance Management (MPM) | <ul style="list-style-type: none"> • Per operationeel en financieel deelgebied zijn er policies; • Pre-SOx-fase; • Controls en compliance zijn gedreven vanuit juridische zaken; • Monitoring van controls is verkokerd en inconsistent; • Performance management monitoring is slechts sporadisch/incidenteel aan de orde. | <ul style="list-style-type: none"> • Mission statement wordt (h)erkend door medewerkers; • Periodieke toetsing van resultaten t.o.v. gestelde doelen (als aparte activiteit) voor monitoring en performance management; • Monitoring en performance management worden onderdeel van normale periodieke rapporteringscyclus; • Afzonderlijke functionarissen in de lijn zien toe op monitoring en performance. |
| Ondersteunende Afdelingen (2e en 3e lijn) (OA) | <ul style="list-style-type: none"> • Niet of in zeer beperkte mate aanwezig; • Afdelingen werken verkokerd en inconsistent; • Afdelingen zijn nog onervaren (in opbouwfase); • Geen periodiek gestructureerd overleg tussen de afdelingen. | <ul style="list-style-type: none"> • Afdelingen raken georganiseerd en er komt een georganiseerde samenwerking tot stand, maar nog reactief; • Er is nog geen duidelijke afbakening tussen de 1e, 2e en 3e lijn ('Three lines of defense'). |

| | Fase 3 | Fase 4 |
|--|--|---|
| | <ul style="list-style-type: none"> • Periodieke toetsing is onderdeel van reguliere controls (niet toegevoegd); • Lijn rapporteert periodiek (over zelfevaluatie) middels bijv. 'Letter of Representation' over naleving van wet- en regelgeving en policies aan hoger management. | <ul style="list-style-type: none"> • Compliance- en control taak geheel in de lijn verankerd; • Organisatie is zelf in staat controls en compliance met interne en externe wet- en regelgeving te toetsen en te borgen; • Testen van controls en compliance ligt geheel in de lijn; • Alleen uitzonderingen worden gerapporteerd. |
| | <ul style="list-style-type: none"> • Continue monitoring en performance management zijn onderdeel van reguliere werkzaamheden (niet toegevoegd) ('war rooms' met zichtbare confrontatie resultaat versus doelstellingen/afspraken); • Hoger management beschikt over (operationeel) dashboard met belangrijkste doelen (en doet hier ook iets mee!). | <ul style="list-style-type: none"> • Compliance- en control taak geheel in de lijn verankerd; • Organisatie is zelf in staat controls en compliance met interne en externe wet- en regelgeving te toetsen en te borgen; • Confrontatie resultaat versus doelstelling ligt geheel in de lijn; • Alleen uitzonderingen worden gerapporteerd via dashboard aan hoger management. |
| | <ul style="list-style-type: none"> • De samenwerking van de afdelingen wordt proactief gemanaged vanuit de RvB; • Afdelingen zijn professioneel en hebben uitmuntende ervaring; • Er is voldoende ruimte en flexibiliteit in de planning van werkzaamheden; • Grenzen tussen 1e, 2e en 3e lijn worden steeds duidelijker. | <ul style="list-style-type: none"> • Afdelingen zijn (voor zover nog aanwezig) zo 'lean & mean' mogelijk en werken optimaal samen met de lijn; • Afdelingen zijn zeer professioneel van opzet; • Er zijn wel duidelijk grenzen in 1e, 2e en 3e lijn; • Er zijn geïntegreerde rapportages over GRC in de onderneming. |

Nederlandse
Beroepsorganisatie
van Accountants



NBA

Antonio Vivaldistraat 2 - 8
1083 HP Amsterdam
Postbus 7984
1008 AD Amsterdam

T: 020 3010301
F: 020 3020302
E: nba@nba.nl
I: www.nba.nl