Voorbeeld van een management control framework voor corporaties

Handreiking 2 bij implementatie Reglement Financieel Beleid en Beheer.

Consultatieversie d.d. 22 juli 2016

Uw reacties op deze consultatieversie zijn van harte welkom. Ook zijn praktische uitwerkingsrichtingen (op onderdelen) welkom.

U kunt die mailen aan:

reactiemodellen@aedes.nl

We zullen uw reacties niet individueel van een antwoord voorzien maar deze verwerken in een volgende versie van deze handreiking die naar verwachting in september zal worden gepubliceerd. Als wij vragen hebben naar aanleiding van uw reactie, nemen wij contact met u op

Aedes vereniging van woningcorporaties

Publicaties

Postbus 29121, 2509 AC Den Haag

088 233 37 00

Inhoud

1. Inleiding: het Management Control Framework

Corporaties hebben doelstellingen die moeten geworden gerealiseerd. Er zijn risico's die het realiseren van die doelstellingen in gevaar brengen. Zowel de doelstellingen als de risico's dienen te worden gemanaged (niet aan toeval over laten). In dit kader kan aansluiting worden gevonden bij een zogenaamd Management Control Framework (MCF), een methodiek die organisaties helpt om hun doelstellingen beter te realiseren en invulling te geven aan beginselen vanuit risicomanagement.

Een goed opgezet en goed werkend MCF borgt dan ook de realisatie van de doelstellingen en compliance tot in de haarvaten van de bedrijfsvoering. Zo helpt het interne toezichthouders en bestuurders hun verantwoordelijkheid te dragen. Gebruik van een MCF sluit bovendien goed aan op de door het Ministerie gekozen uitgangspunten[1], die uitgaan van een systeemaanpak, zoals ook de kerngedachte is van een MCF.

1.1. Doelstelling MCF

Het MCF is een middel in het kader van de interne beheersing. De definitie van interne beheersing kan als volgt voor de corporatiesector worden vertaald:

Een proces geïnitieerd en gerealiseerd door de RvC en bestuurder van een corporatie met als doel een redelijke mate van zekerheid te verkrijgen om de doelstellingen te bereiken op het gebied van:

1. *een efficiënte en effectieve bedrijfsvoering om de volkshuisvestelijke doelstellingen te realiseren, met als randvoorwaarde het waarborgen van de financiële continuïteit;*
2. *een betrouwbare financiële verslaggeving;*
3. *voorkomen van misbruik en oneigenlijk gebruik van wettelijke regelingen.*

Uit deze definitie blijkt dat interne beheersing een verantwoordelijkheid is van iedereen die werkzaam is binnen de corporatie. Het is dus niet alleen een verantwoordelijkheid van het (top)management, maar ook van afdelingshoofden, coördinatoren en medewerkers op ieder niveau in de organisatie. Het doel van een MCF is zeker te weten dat alle medewerkers bijdragen aan het realiseren van de doelstellingen. De doelrealisatie hangt met een MCF voor de corporatie minder van het toeval af.

De term Management Control Framework bestaat uit:

- *Management Control*: in het kader van Corporatie Governance is het belangrijk dat de RvC en het bestuur zichtbaar en achteraf bewijsbaar in control zijn ("Management Control").
- Framework: in de kern is een Control Framework een set van samenhangende (vandaar "framework") maatregelen.

Dat is in elke organisatie belangrijk, maar voor corporaties geldt dit in versterkte mate gezien de publieke functie. De leden van de RvC en de bestuurders hebben ook een persoonlijk belang bij een MCF. Bestuurders en commissarissen mogen immers door de corporatie op grond van de woningwet niet worden gevrijwaard voor hun bestuurlijke aansprakelijkheid.

1.2. MCF: niet verplicht

Uiteraard is iedere corporatie vrij om zijn eigen MCF systeem te kiezen of dat achterwege te laten. Sterker nog: de Woningwet verplicht niet tot het hanteren van een MCF. Echter, gezien de toenemende complexiteit in de omgeving waarin corporaties acteren, de wettelijke eisen die worden gesteld aan een corporatie en de hoeveelheid van stakeholders waar de corporatie rekening mee moet houden, is een MCF op termijn wenselijk, mogelijk zelfs een "must" om ondanks de complexiteit, de eigen volkshuisvestelijke doelstellingen "gemanaged" te realiseren.

1.3. Ondersteuning Aedes en VTW

Aedes en VTW willen graag ondersteuning bieden aan de sector die voor de uitdaging staat om te moeten voldoen aan een risicogerichte systeemaanpak betreffende de inrichting van de bedrijfsactiviteiten, het uitvoeren van het toezicht en het afleggen van verantwoording. Met deze handreiking presenteren Aedes en VTW een voorzet voor een MCF uitgaande van de bekende en breed geaccepteerde COSO-methodiek. Daarbij is van belang aan te geven dat Aedes en VTW geen voorkeur

[1] Voor meer achtergrondinformatie zie: publicatie Aedes en VTW: Positionering van het Reglement financieel beleid en beheer, sturing activiteiten en modelstatuten.

hebben voor een bepaald MCF model. Maar om het een en ander concreet te maken is wel gekozen om het COSO- model als leidraad te nemen.

In het uitgewerkte MCF (hoofdstuk 2 en verder) is een voorzet gegeven voor een verdere invulling bij de corporatie. In een getailleerde bijlage (zie excel) is op basis van een kleine 100 aspecten aangegeven hoe de verdere praktische invulling kan zijn.

1.4. Doorontwikkelen MCF

Het MCF is een relatief nieuw fenomeen in de corporatiesector. Uit navraag door Aedes en VTW leert dat nog maar weinig corporaties een MCF daadwerkelijk in de volle breedte hebben geïmplementeerd. De implementatie van een MCF zal een traject zijn dat meerdere jaren beslaat. Wel zal blijken dat als een corporatie er mee aan de slag gaat, veel onderdelen reeds binnen de organisatie zijn geborgd. Het MCF is immers een kapstok waarin alle onderwerpen op een gestructureerde manier geordend kunnen worden. Bovendien wordt dan ook zichtbaar waar nog “blinde vlekken” zijn. De corporatie kan vervolgens zelf kiezen waar de aandacht op gevestigd gaat worden voor doorontwikkeling. Zo ontstaat er een overzicht en inzicht.

Maar ook voor Aedes en VTW is dit een eerste aanzet. Vandaar dat opmerkingen, aanmerkingen en uitwerkingsrichtingen (voor onderdelen) van harte welkom zijn zodat kennis rond het fenomeen MCF voor corporaties sectorbreed kan worden gedeeld. Immers niet elke corporatie hoeft het wiel opnieuw uit te vinden.

En nogmaals, alles op vrijwillige basis, niets moet!

2. Management Control Framework: COSO

In dit hoofdstuk volgt een nadere uitwerking van een MCF voor de corporatiesector. Bij de inrichting van een MCF kunnen verschillende benaderingen worden gehanteerd. Hier geval is gekozen voor COSO. Belangrijk is op te merken dat de inrichting van een MCF maatwerk is en corporatie-specifiek.

2.1. Waarom COSO?

Voor het MCF zijn er meerdere concepten bekend. Een werkgroep van Aedes heeft met name de volgende modellen overwogen: COSO, de “levers of control van Simons”, het “3 lines of defence model” en de “Golden Circle” van Simon Sinek. Niet een van de modellen is “goed of fout”.
De werkgroep heeft overwogen dat het belangrijk was een MCF te kiezen dat zijn waarde heeft bewezen en naar verwachting bekend zal zijn bij een (groot) aantal van de leden. Ook is duidelijk dat de corporaties zich in een tijd bevinden waarin de “hard controls” dominant zijn. Compliance staat voorop. De soft controls (cultuur) zijn erg belangrijk, maar vooral ondersteunend. Ook de flexibiliteit in het MCF is belangrijk. Het MCF moet ruimte bieden aan andere concepten.

In het voorbeeld MCF is voor uitwerking via de lijnen van COSO gekozen omdat het een wereldwijd al vele jaren (sinds 1992) beproefd concept is dat ook op universiteiten wordt gedoceerd. De keuze voor COSO is herkenbaar voor de medewerkers van de corporaties die belast zijn met vraagstukken op het gebied van governance. COSO is robuust en biedt ruimte om andere visies in te passen. COSO biedt hierdoor de mogelijkheid tot maatwerk. Uiteraard staat het de corporatie vrij een MCF uit te werken via een ander concept.

2.2. Wat is COSO?

COSO is een MCF dat is ontwikkeld door The Committee of Sponsoring Organizations of the Treadway Commission (COSO). Dit comité, bestaande uit een aantal private organisaties, heeft in 1992 naar aanleiding van een aantal boekhoudschandalen en fraudegevallen aanbevelingen gedaan en richtlijnen aangegeven ten aanzien van interne controle en interne beheersing. De doelstelling van COSO was en is om een wereldwijd verbreid kader te scheppen aan de hand waarvan interne beheersing (of *internal control*) kan worden beoordeeld. In deze eerste versie uit 1992 is ook, voor het eerst, een breed onderschreven definitie opgenomen van het begrip internal control (Interne beheersing).

2.3. De Kubus: 5 componenten

COSO bestaat uit vijf met elkaar verbonden componenten met als doelstelling zekerheid over de realisatie van de strategische doelstellingen van de organisatie te bereiken:

1. *Control Environment* (interne beheersomgeving)
   Het fundament van interne sturing en beheersing. Dit omvat onder andere de normen en waarden van de organisatie, de integriteit en gedragingen van management en werknemers, de organisatiestructuur en hoe bevoegdheden zijn verdeeld.
2. *Risk assessment* (risicobeheersing)
   De identificatie van voor de organisatiedoelstellingen relevante risico’s.
3. *Control activities* (interne beheersmaatregelen)
   Het beleid en de procedures die waarborgen dat de instructies van het management worden uitgevoerd en die bewaken dat de risico’s op de organisatiedoelstellingen worden beheerst.
4. *Information and communication* (informatie en communicatie)
   De communicatie van management naar werknemers over de uit te voeren procedures en de communicatie van alle van belang zijnde informatie richting management. Deze betreft niet alleen interne informatie, maar ook informatie over ontwikkelingen buiten de organisatie.
5. *Monitoring* (monitoring activiteiten)
   Het proces van vaststellen of maatregelen voldoende effectief zijn geweest.

Het COSO-model is wereldwijd bekend door de volgende kubus:

Aan de voorkant van de kubus zijn de 5 bovengenoemde componenten opgenomen (interne beheersomgeving, risicobeheersing, de interne beheersmaatregelen , informatie en communicatie en de monitoring activiteiten). Op de bovenkant van de kubus staan de 3 doelstellingen: bedrijfsvoering (operations), verslaggeving (reporting) en compliance. De 3e dimensie van de kubus geeft aan dat COSO bedoeld is om op elk organisatieniveau uit te werken. In deze handreiking wordt het uitgewerkt tot op corporatieniveau (“entity-level).

2.4. Corporatie-specifiek

Het COSO framework wordt in deze handreiking vertaald naar en concreet gemaakt voor de corporatie-sector. In de bijlage (excel) is een tabel opgenomen aan de hand waarvan elke corporatie tot op detailniveau (bijvoorbeeld niveau van documenten) een MCF kan uitwerken. In de tabel worden per item onderwerpen benoemd waaraan kan worden gedacht en er wordt verwezen naar voorbeelden. Te denken valt hierbij bijvoorbeeld aan de Aedes gedragscode en het model voor de beoordeling van de risico’s door het WSW.

3. Nadere uitwerking van: COSO

Hier volgt een nadere uitwerking van het COSO model, specifiek voor de corporatiesector. Het COSO-model kent 5 componenten die weer onderverdeeld worden in 17 principes. Deze principes kunnen weer verder worden uitgewerkt in 81 attributen. In deze Aedes-handreiking MCF zijn deze componenten alle beschreven en hiermee voor toepassingen binnen de corporatiesector inzichtelijk gemaakt. Het is verstandig om naast deze handreiking ook de excelbijlage (schema) uit te printen en bij de hand te houden zodat makkelijk het overzicht behouden blijft.

(paragraaf 3.1) Component 1: De interne beheersomgeving: 5 principes:

1) Commitment met integriteit en ethische waarden.
2) Bestuur en toezicht zijn onafhankelijk van het management en houden toezicht op de inrichting en werking van de interne beheersing.
3) Organisatie- en verantwoording structuur met de bijbehorende verdeling verantwoordelijkheden, taken en bevoegdheden.
4) Adequaat HRM.
5) Bevorderen van de lijnverantwoordelijkheid voor interne beheersing.

(paragraaf 3.2) Component 2: Risicobeheersing: 4 principes:

6) Bepalen van SMART geformuleerde doelen.
7) Identificatie en analyse van risico´s met betrekking tot de realisatie van de doelen.
8) Bewustzijn van frauderisico´s.
9) Identificatie en beoordeling van veranderingen die de interne beheersing significant beïnvloeden.

(paragraaf 3.3) Component 3: beheersingsmaatregelen: 3 principes:

10) Selectie en ontwikkeling van beheersingsmaatregelen voor de mitigatie van risico's.
11) Selectie en ontwikkeling van algemene beheersingsmaatregelen over (IC)T.
12) Beheersingsmaatregelen zijn gebaseerd op beleid en worden uitgewerkt in adequate procedures.

(paragraaf 3.4) Component 4: informatie en communicatie: 3 principes:

13) Inrichting van een adequate informatievoorziening voor de ondersteuning van de interne beheersing.
14) Inrichting van een ondersteunende interne communicatiestructuur.
15) Inrichting van een externe communicatiestructuur.

(paragraaf 3.5) Component 5: Monitoring activiteiten: 2 principes:

16) Inrichten en uitvoeren van continue of periodieke evaluatie van het bestaan en de werking van de interne beheersingsmaatregelen.
17) Tekortkomingen in de interne beheersing worden tijdig gerapporteerd aan partijen die verantwoordelijk zijn voor correctieve maatregelen.

In de volgende paragrafen zullen we de vijf componenten en 17 principes verder op hoofdlijnen uitwerken. Aangezien dit een eerste aanzet is vanuit Aedes en VTW zijn aanvullingen, opmerkingen etc. van harte welkom.

3.1. De interne beheersomgeving: 5 principes (1 t/m 5)

De interne beheersomgeving is het fundament van interne sturing en beheersing. Het fundament omvat onder andere de normen en waarden van de organisatie, de integriteit en gedragingen van management en werknemers, de organisatiestructuur en hoe bevoegdheden zijn verdeeld. De interne beheersomgeving determineert de opzet van het MCF. Hierna worden de vijf principes gedefinieerd en nader uitgewerkt. Ook wordt de relatie gelegd met de Governancecode Woningcorporaties 2015 die in belangrijke mate langs dezelfde lijnen is opgebouwd.

Principe 1: commitment met integriteit en ethische waarden

De corporatie stelt de kernwaarden vast en houdt deze levend in de organisatie door hier bewust mee om te gaan. De corporatie kan bij de bepaling van de kernwaarden aansluiten op de door Aedes samen met de leden ontwikkelde visie op de toekomst van de corporaties.

Voorbeeldgedrag van de hoogste leiding is erg belangrijk om de kernwaarden in de organisatie te internaliseren. De RvC heeft een cruciale rol bij het scherp houden van de bestuurder op zijn voorbeeldgedrag. De bestuurder heeft deze cruciale rol naar de organisatie van de corporatie. De *interne* beheersomgeving voor het principe *Commitment met integriteit en ethische waarden* zal door corporaties worden geoperationaliseerd. De Aedes gedragscode is hiervoor goed bruikbaar. Deze kan door de RvC worden vastgesteld. Vanzelfsprekend moet de corporatie aandacht besteden aan de invoering en het levend houden van de gedragscode door bijvoorbeeld dilemma trainingen en structurele opname in de HRM

beoordelingssystemen. De bestuurder kan jaarlijks de naleving van de gedragscode evalueren en daarover de bevindingen rapporteren aan de RvC. Het is belangrijk dat deze gedragscode bij de corporatie is geïnternaliseerd en echt leeft op alle niveaus door hier veelvuldig over te communiceren. Het gaat hier immers om het ethische DNA van de corporatie. Tot slot moet de corporatie tijdig niet-naleving vaststellen en herstellen. Hiertoe stelt de RvC een klokkenluidersregeling vast en wordt deze op de website gepubliceerd.

De uitwerking van het MCF sluit rond dit principe aan op de governancecode Woningcorporaties 2015 (hierna: governancecode). Deze governancecode kent 5 uitgangspunten (lees: principes) waarvan de eerste is:

"Uitgangspunt 1 governancecode: Leden van bestuur en RvC hanteren waarden en normen die passen bij de maatschappelijke opdracht.

Voor bestuur en RvC staat het behalen van maatschappelijke resultaten voorop. Dat vraagt om organisaties met een integere en open cultuur waarbinnen ruimte is voor reflectie en tegenspraak. Bestuur en RvC vervullen daarbij een voorbeeldfunctie voor zowel hun eigen corporatie als voor de gehele sector. "

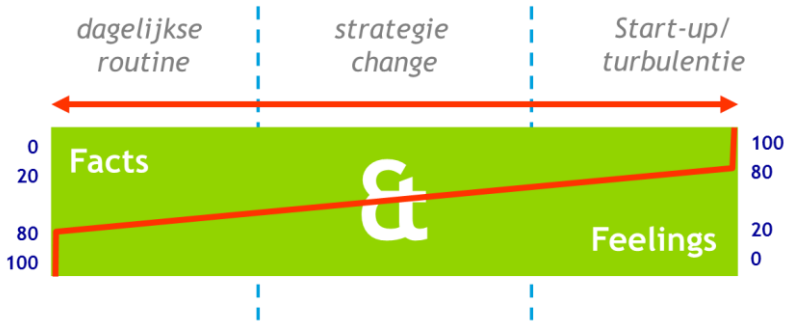
Principe 2: bestuur en toezicht zijn onafhankelijk van het management en houden toezicht op de inrichting en werking van de interne beheersing

Corporaties hebben wettelijk een intern toezichthoudend orgaan, namelijk de RvC[2]. De RvC moet voor het toezicht de verantwoordelijkheden, taken en bevoegdheden vaststellen en toedelen. Daarnaast moet worden nagedacht welke expertises nodig zijn. Het is zelfs wettelijk voorgeschreven dat wordt gewaarborgd dat de RvC voldoende kennis heeft van financieel beleid en beheer (BTIV art. 105 lid sub f). Zie ook het reglement financieel beleid en beheer. De uitwerking van het MCF op dit principe sluit aan op de governancecode. Deze governancecode kent 5 uitgangspunten waarvan het derde is:

"Uitgangspunt 3 governancecode: Bestuur en RvC zijn geschikt voor hun taak.

Het vervullen van de maatschappelijke opdracht van woningcorporaties vraagt om deskundige bestuurders en toezichthouders, die permanent investeren in hun kennis en kunde. Daartoe moeten bestuur en RvC zodanig zijn samengesteld dat de leden elkaar aanvullen en scherp houden."

Bij de bepaling van de benodigde expertise geldt in de basis dat bij toezicht op corporaties in een turbulente omgeving er meer aandacht moet zijn voor niet direct meetbare en zichtbare factoren en andersom.



Het is daarnaast verstandig dat de kwaliteit van de RvC in evenwicht is met de behoefte aan toezicht bij de corporatie. Ook moet de ervaring van de RvC in balans zijn met de kennis van de corporatiesector.

Een belangrijke taak van de RvC is het organiseren van toezicht op de interne beheersing (beleid, richtlijnen en beoordeling). De RvC moet een toetsingskader vaststellen. Hier zijn al veel voorbeelden voor ontwikkeld. De meest vergaande en "mooie" wijze om het toezicht op de interne beheersing te regelen is het vragen van een In Control statement van de bestuurder. Een in control statement is een verklaring van een bestuurder dat hij in control is. Afgifte van een In-control statement door het bestuur vereist dat alle belangrijke processen binnen de organisatie worden beheerst. Een in-control statement kan dus uitsluitend tot stand komen als uitvloeisel van gerichte inspanningen door alle leden van de organisatie. Met andere woorden: alle afdelingen moeten in control zijn (een eigen in control statement kunnen afgeven) waarop het in-control statement van de bestuurder is gebaseerd. De bestuurder is evenwel verantwoordelijk voor

[2] RvC: kan ook RvT heten, maar hier wordt het begrip RvC gehanteerd.

de implementatie van een dergelijke systematiek en zal derhalve een initiërende rol moeten vervullen waarover hij verantwoording aflegt aan zijn interne toezichthouder.

De uitwerking van het MCF op dit principe sluit aan op de governancecode. Deze governancecode kent 5 uitgangspunten waarvan het vijfde is:

"Uitgangspunt 5 governancecode: Bestuur en RvC beheersen de risico's verbonden aan hun activiteiten.
Woningcorporaties hebben te maken met grote (financiële) risico's. Het bestuur is verantwoordelijk voor goede risicobeheersing en de RvC houdt hierop toezicht. Het gaat daarbij niet alleen om de harde beheersmaatregelen maar ook om maatregelen die appelleren aan het risicobesef en de moraal binnen de corporatie".

De RvC laat zich door de bestuurder informeren over de score van de corporatie op het risicomanagement systeem, waarin ook aansluiting is gemaakt met het risicomanagement systeem van het WSW.

Het is ook noodzakelijk de onafhankelijkheid van het toezicht te waarborgen. In het reglement voor de RvC wordt geregeld op welke wijze de RvC de onafhankelijkheid van het toezicht waarborgt.

Principe 3: organisatie- en verantwoording structuur met de bijbehorende verdeling verantwoordelijkheden, taken en bevoegdheden
De verantwoordelijkheid voor de inrichting van deze structuur ligt bij de bestuurder. Vanzelfsprekend moet de RVC wel toezien op de keuzes van de bestuurder. De keuzes van de bestuurder moeten logisch samenhangen, voldoen aan de statuten van de corporatie en tevens aan de wettelijke bepalingen, aansluiten op de processen, een passende span of control hebben en rekening houden met juridische vereisten. Als voorbeeld moet het doel en nut van het hebben van een holdingstructuur voor de RvC duidelijk zijn. De RvC kan in dit kader een verbindingenstatuut vaststellen.

Voorbeeld waarover op hoofdlijnen uitspraken kunnen worden gedaan zijn het opdrachtgeverschap, Kiest de corporatie wel of niet voor ketensamenwerking, wordt gekozen voor een eigen onderhoudsdienst en wil de corporatie al dan niet een "regiecorporatie" zijn.

De RvC toetst of de gekozen organisatiestructuur voldoende waarborgen biedt voor een integere bedrijfsvoering (denk aan toereikende controletechnische functiescheiding). Er is sprake van een toereikende controletechnische functiescheiding als de functies beschikken, bewaren en registreren zijn gescheiden in de processen. De wettelijk verplichte controlfunctie (> 2.500 eenheden) toetst de werking van de functiescheiding.

De RvC moet ook (laten) toetsen dat de door de bestuurder gekozen structuur de RvC kan voorzien van de voor haar toezicht benodigde informatie. Bovendien heeft de RvC een wettelijk geregelde actieve informatieplicht richting de minister (artikel 29 BTIV). Dit is een belangrijk punt in relatie tot de aansprakelijkheidsrisico's van de leden van de RvC en de

bestuurder. Verder moet zijn geborgd dat de RvC toegang heeft tot alle informatie die relevant is voor haar toezicht. Sommige corporaties kiezen ervoor dat de RvC haar eigen secretariaat heeft.

De RvC toetst ook de opzet van de informatiestromen. “Minder is meer” is hierbij het motto. De RvC streeft naar een informatiestructuur waarbij de informatievoorziening van de bestuurder aansluit op het toetsingskader van de RvC. Concreet betekent dit dat de bestuurder in de loop van het jaar met name rapporteert over de in het toetsingskader door de RvC benoemde punten (denk aan maximaal 10). Bijvoorbeeld maatschappelijke legitimiteit, relatie met de gemeente, aantal bereikbare woningen. In het sturingsmodel zijn de punten die voor het toetsingskader in aanmerking komen uitvoerig uitgewerkt. Een eerste aanzet van het sturingsmodel is uitgewerkt in de bijlage van handreiking 1 bij de implementatie van het reglement financieel beleid en beheer. Voor de lopende zaken kan de RvC in het toetsingskader regelgrenzen vast stellen. De bestuurder rapporteert dan slechts als de regelgrens wordt overschreden. Een regelgrens kan bijvoorbeeld zijn 5 % van de personeelskosten. Onderschrijdingen tot 95 % en overschrijding tot 105 % van het budget zijn de verantwoordelijkheid van de bestuurder die jaarlijks achteraf verantwoording aflegt aan de RvC. De RvC laat de werking van de rapportage door de bestuurder conform het toetsingskader controleren door de accountant (optioneel).

Principe 4: adequaat HRM

De bestuurder moet zorg dragen voor een aansluiting tussen het beleidsplan en de verantwoordingsformatie. Een regiecorporatie heeft minder medewerkers in dienst dan een corporatie die er voor kiest alle taken in eigen beheer uit te voeren. De kern van het HRM-principe is dat de bij het personeel aanwezige competenties aansluiten bij de behoeften van de corporatie. “De juiste mens op de juiste plek”. Hoe gaat de corporatie om met het nieuwe / flexibele werken? De bestuurder moet formuleren op basis van de strategische doelstellingen van de corporatie welke competenties de corporatie terug wil zien bij het personeel. Een innovatieve technologische corporatie heeft andere mensen nodig dan een kleine beheercorporatie Ook zijn er kleine corporaties die voornamelijk bestaan uit vrijwilligers.

Tot slot is voor elke corporatie van belang te zorgen dat het personeel zich kan blijven ontwikkelen en op de hoogte is van wijzigingen in wet en regelgeving alsook op de hoogte wat de betekenis is van de visie, missie en strategie voor hun specifieke werkzaamheden. De corporatie moet instrumenten hebben zoals een Management development plan, persoonlijke ontwikkelingsplannen, cultuurmeting e.d. De RvC volgt kritisch het door de bestuurder voorgestelde en bestede opleidingsbudget voor het personeel in relatie tot de na te streven doelstellingen uit het beleidsplan.

De bestuurder legt het HRM beleid vast in een HRM beleidsplan en richtlijnen. Onderdeel hiervan is gestructureerde aandacht voor de werving, selectie, opleiding en binding van voldoende competent personeel. Jaarlijks wordt het HR-beleid geëvalueerd en door de bestuurder met de RvC besproken. Bij deze evaluatie heeft de RvC met name aandacht voor het management development van mensen op sleutelposities van belang voor de Interne Beheersing zoals de controlfunctie.

De strategische uitgangspunten van HR kunnen worden uitgedrukt in kernwaarden. Daarnaast kan een corporatie het belangrijk vinden dat de medewerkers geëngageerd zijn, integer handelen , goed kunnen samenwerken, voldoende beslissingsruimte hebben, proactief zijn, zelf initiatief nemen, flexibel en kostenbewust zijn. Dit kan weer worden doorvertaald naar concrete gedragsnormen.

Principe 5: bevorderen van de lijnverantwoordelijkheid voor interne beheersing

De bestuurder zorgt voor bewustzijn bij het lijnmanagement voor interne beheersing. Hij kan bijvoorbeeld er voor kiezen aan elke lijnmanager een in control statement te vragen. Ook is het belangrijk dat hij de lijnmanagers er van bewust maakt dat zij verantwoordelijk zijn voor bevindingen van de controlfunctie of de accountant. Het is noodzakelijk dat de gekozen doelstellingen vanuit het bestuur worden doorvertaald naar de werkvloer voor de concrete actie. De bestuurder is verantwoordelijk, maar uiteindelijk komt het gewenste resultaat – de organisatie is in control - er alleen als een resultante van inspanningen door de gehele organisatie.

Uiteindelijk zijn het de medewerkers “die het moeten doen”. De beoordelings- en beloningscriteria van het personeel van de corporatie moeten aansluiten op de kritische succesfactoren. Met andere woorden: het personeel moet (passend) worden beloond en incentives krijgen voor die prestaties die bijdragen aan de realisatie van de doelstellingen van de corporatie. De bestuurder moet verantwoording afleggen aan de RvC of en hoe hij de lijnverantwoordelijkheid voor de interne beheersing heeft geëvalueerd.

3.2. Risicobeheersing: 4 principes (6 t/m 9)

Voor het toezicht van de RvC op de risicobeheersing zijn de oordelen van externe partijen relevant: de Autoriteit Woningcorporaties, het WSW, de gemeenten en de huurdersorganisaties. WSW hanteert een risicomodel dat onderdeel kan zijn van de interne risicobeheersing. Tevens kunnen hierbij de resultaten uit de Aedes-benchmark worden betrokken omdat deze resultaten een spiegel voor de bedrijfsvoering van de corporatie zijn. Ook het 4-jaarlijks verplichte visitatierapport is voor de RvC een belangrijke spiegel. De RvC ziet er op toe dat de bestuurder de juiste focus heeft bij zijn risicomanagement. Het moet om het beheersen van die risico's gaan die het bereiken van de doelstellingen in gevaar brengen. Risicobeheersing heeft als doel deze bedreigende factoren te identificeren, de kans en impact van optreden vast te stellen en te bepalen op welke wijze met deze risico's kan worden omgegaan: vermijden, overdragen, accepteren of beperken zijn de wijzen waarop kan worden gereageerd.

Principe 6: Bepalen van SMART geformuleerde doelen

De bestuurder is er verantwoordelijk voor dat binnen de corporatie de doelstellingbepaling SMART plaatsvindt. Deze doelen moeten aansluiten op de strategische doelstellingen ("alignment"') . Daarnaast moet de corporatie voldoen aan doelen die worden opgelegd door externe regelgeving ('compliance"). Het bestuur moet een keuze maken over de risico tolerantie ook wel "risk appetite", zijnde de mate van risico´s die de bestuurder bereid is te nemen. Met andere woorden: op welk moment is een afwijking van een doel een bedreiging voor het realiseren van de strategische doelstellingen? De RvC houdt toezicht op de logische samenhang van de keuzes van de bestuurder.

Principe 7: Identificatie en analyse van risico´s met betrekking tot de realisatie van de doelen

De bestuurder kan bepalen welke interne en externe factoren en gebeurtenissen een bedreiging kunnen zijn voor de realisatie van de doelstellingen van de corporatie. De bestuurder brengt in beeld de kans van optreden en de impact-schade. Deze analyse kan worden vastgelegd en besproken met de RvC.

De bestuurder analyseert de risico's op significantie. Risico's kunnen zich bevinden op het strategische, tactische en operationele niveau. De bestuurder kan mede op basis van de analyse de respons (aanvaarden, vermijden, verminderen of delen) bepalen op de analyse zoals vastgelegd in de "Risico-map", waaronder een impactanalyse. Met name de risico's op strategisch en tactisch niveau zullen besproken worden tussen bestuur en RvC. In veel gevallen zijn externe risico's bepalend. In dit kader kan het raadzaam zijn om vooraf inschattingen te maken in de vorm van scenario-analyses.

Principe 8: Bewustzijn van frauderisico´s

Elke administratieve organisatie kent inherent het risico van fraude. Fraude kan nooit worden uitgesloten. De bestuurder kan een frauderisico-analyse laten maken waarin hij analyseert waar zwakke plekken in de organisatie zitten en wellicht perverse prikkels in de primaire processen zijn opgenomen. Ook geeft hij aan welke maatregelen hij heeft genomen om fraude zoveel mogelijk uit te sluiten en te voorkomen. De bestuurder geeft jaarlijks opdracht aan de controlfunctie van de corporatie om de frauderisico-analyse op te stellen. Deze frauderisicoanalyse kan worden beoordeeld door de RvC in aanwezigheid van de controlfunctie. In de frauderisico-analyse kan door de bestuurder in ieder geval aandacht worden besteed aan de volgende aspecten:

- diefstal, valsheid in geschrifte en corruptie.
- Risico's op datalekken en aangaande cybersecurity.
- De significantie van de schade en de impact op de managementinformatie en compliance.
- De invloed van incentives en andere beïnvloeding.
- De zwakke plekken in de processen (activa en rapportages).
- De houding van de organisatie ten opzichte van rationalisatie van normafwijkend gedrag.
- De cultuur in relatie tot fraude.

Principe 9: Identificatie en beoordeling van veranderingen die de interne beheersing significant beïnvloeden

Het gaat hier om *veranderingen* in de visie , missie en strategie van de corporatie, politieke opvattingen, externe wet en regelgeving, veranderingen in het business model en veranderingen in het management. Veranderingen in de externe regelgeving dienen vroegtijdig te worden gesignaleerd. Daarom is het belangrijk dat zowel de RvC, het bestuur maar ook de medewerkers, de informatievoorziening door Aw, MinBZK, WSW, Aedes en de VTW nauwlettend volgen.

Het business model moet de RvC goed doorgronden en zo nodig zich door de bestuurder diepgaand laten informeren. Het business model gaat over de vraag hoe de corporatie haar geld verdient. Dit betreft de missie, de strategie en de producten en diensten die de corporatie aanbiedt. Pas als de RvC het businessmodel goed begrijpt kan de RvC goed toezicht houden.

De RvC moet derhalve alert zijn op veranderingen in het businessmodel omdat die veranderingen moeten leiden tot toezicht op andere, nieuwe punten. Een concreet voorbeeld is de introductie van de verhuurderheffing. Dit had nogal wat impact op het businessmodel van de corporaties. Van belang is dat op dat moment het gesprek wordt opgestart tussen bestuur en RvC over hoe hier mee om te gaan en aan “welke knoppen” wordt gedraaid om de financiële continuïteit opnieuw te borgen en het businessmodel weer duurzaam te maken.

Veranderingen in het management is een aspect waar de RvC vanzelfsprekend in detail over moet worden geïnformeerd en waar deze in bepaalde gevallen initiërend is.

3.3. Beheersingsmaatregelen: 3 principes (10 t/m 12)

De corporatie heeft strategische doelstellingen. Deze doelstellingen dienen te worden gerealiseerd. Deze doelrealisatie moet worden beheerst. Er zijn factoren die het bereiken van deze doelstellingen in gevaar brengen. De corporatie heeft deze bedreigende factoren in beeld gebracht bij *Component 2. Risicobeheersing*. Nu kan de corporatie de *maatregelen* bepalen die de corporatie wil invoeren. Dit alles met als doel de realisatie van de strategische doelstellingen te waarborgen.

De component beheersingsmaatregelen is door COSO in 3 principes verder uitgewerkt:

1. selectie en ontwikkeling van beheersingsmaatregelen voor de mitigatie van risico's.
2. Selectie en ontwikkeling van algemene beheersingsmaatregelen over (IC)T.
3. Beheersingsmaatregelen zijn gebaseerd op beleid en worden uitgewerkt in adequate procedures.

Principe 10: Selectie en ontwikkeling van beheersingsmaatregelen voor de mitigatie van risico's

De te kiezen beheersingsmaatregelen moeten in lijn zijn met de gemaakte keuzes voor risicotolerantie / risk appetite. Zie hier ook de relatie met het risicomodel van het WSW. De te kiezen beheersingsmaatregelen moeten passend zijn voor de relevante bedrijfsprocessen (“niet met een kanon op een mug schieten”). Tot slot moeten de te kiezen beheersingsmaatregelen aansluiten op de specifieke situatie. Zo zijn beheersingsmaatregelen voor verkoop van woningen bij een corporatie die alle woningen in bezit houdt zinloos. Andere belangrijke opties zijn of de beheersingsmaatregelen handmatig dan wel zoveel mogelijk geautomatiseerd worden uitgevoerd en ook of de corporatie kiest voor preventief (vooraf) of detectief (achteraf). Vanzelfsprekend moet ook de minimaal noodzakelijke controletechnische functiescheiding worden aangebracht. De bestuurder vraagt de controlfunctie om de risicomaatregelen te toetsen op aansluiting op “wat er speelt ”bij de corporatie. Dit is belangrijk omdat hiermee wordt geborgd dat de beheersingsmaatregelen leven in de organisatie en als nuttig worden ervaren.

Principe 11: Selectie en ontwikkeling van algemene beheersingsmaatregelen over (IC)T

Technologie is een belangrijk onderdeel voor de bedrijfsvoering van corporaties. De bestuurder zal een beeld hebben van het antwoord op de vraag of en in hoeverre de bedrijfsprocessen afhankelijk zijn van de technologie (IT). Deze afhankelijkheid bepaalt de mate en intensiteit van de maatregelen die de corporatie moet nemen om de werking van de IT te waarborgen. Te denken valt aan privacyrisico’s in relatie tot werken in de “cloud’ en de waarborging van de vertrouwelijkheid van de inkomens gegevens van de huurders. Daarnaast de traditionele vragen zoals logische toegangsbeveiliging, functiescheiding en backup en recovery. Denk ook aan functiescheiding tussen de gebruikers-organisatie, de IT organisatie en de beheerorganisatie.

IT gaat vaak om materiele bedragen. Daar komt bij dat IT specifieke deskundigheid vereist. De RvC kan er op toezien dat de bestuurder deze complexe materie op adequate wijze weet te beheersen. Denk bijvoorbeeld aan het door de RvC inzetten van een extern deskundige specifiek voor de toetsing van de waarborging van de kwaliteit en de betrouwbaarheid van het IT systeem. De RvC zal er op toezien dat de bestuurder de sector kennis van de data architectuur goed benut. “CORA en VERA” zijn de begrippen die besproken kunnen worden tussen de bestuurder en de RvC.

Principe 12: Beheersingsmaatregelen zijn gebaseerd op beleid en worden uitgewerkt in adequate procedures

Hiervoor zijn de beheersingsmaatregelen gekozen. Het gaat er nu om deze beheersingsmaatregelen goed in te bedden in de organisatie van de corporatie. In deze fase worden verantwoordelijkheden, taken en bevoegdheden vastgesteld en vastgelegd in procedures en functiebeschrijvingen. De bestuurder kan vaststellen dat de mensen die de beheersings-maatregelen gaan uitvoeren ter zake deskundig en toegewijd zijn. Ook zal de bestuurder door de controlfunctie (laten) vaststellen dat de beheersingsmaatregelen tijdig en conform vastgestelde procedures worden uitgevoerd. Hiertoe wordt een intern controle plan vastgesteld door de bestuurder en ter goedkeuring aan de RvC voorgelegd.

Essentieel is dat gesignaleerde onvolkomenheden worden omgezet in passende acties. Het actie ondernemen op basis van gesignaleerde onvolkomenheden is relevant voor de RvC om kennis van te nemen. Het is namelijk een belangrijke indicatie van de mate waarin de bestuurder in control is.

Tot slot moet de bestuurder de beheersingsmaatregelen periodiek evalueren en deze evaluatie ter beoordeling aan de RvC voorleggen.

3.4. Informatie en communicatie: 3 principes (13 t/m 15)

De corporatie legt als maatschappelijke onderneming aan diverse stakeholders verantwoording af over haar werkzaamheden. Voor het afleggen van verantwoording is een adequate informatievoorziening nodig. Dilemma's hierbij zijn met name de volledigheid en toegankelijkheid en de juistheid en tijdigheid. De component informatie en communicatie is door COSO in 3 principes verder uitgewerkt:

1) inrichting van een adequate informatievoorziening voor de ondersteuning van de interne beheersing.
2) Inrichting van een ondersteunende interne communicatiestructuur.
3) Inrichting van een externe communicatiestructuur.

Principe 13: Inrichting van een adequate informatievoorziening voor de ondersteuning van de interne beheersing

De informatievoorziening moet passend zijn. Teveel of te weinig informatie is in beide gevallen niet de bedoeling. De praktijk is dat er wel informatie bijkomt, maar niet afgaat. Daarom is het nuttig om periodiek stil te staan bij de informatiebehoefte met de vraag "wat kan er af?". De informatie die wordt verstrekt moet voldoen aan kwaliteitseisen zoals juistheid, tijdigheid, volledigheid, relevantie en inzichtelijkheid. Om mogelijk te maken dat informatie wordt gegenereerd moeten gegevens worden verzameld. Hiervoor moeten de juiste systemen aanwezig zijn.

De RvC kan bijvoorbeeld jaarlijks een toetsingskader op stellen tav de informatievoorziening. De bestuurder rapporteert aan de RvC conform dat toetsingskader. De bestuurder op zijn beurt bepaalt op basis van de geïdentificeerde risico's, de bijbehorende maatregelen en regelgrenzen op welke wijze hij door het lijn management wordt geïnformeerd over de bedrijfsprocessen.

De bestuurder beoordeelt of en in hoever de informatievoorziening aansluit op CORA (de corporatie-referentie architectuur).

De bestuurder vraagt de controlfunctie jaarlijks separaat de kosten en baten van de informatieverstrekking te analyseren op passendheid bij de doelrealisatie. De controlfunctie bespreekt zijn bevindingen met de Bestuurder.

Principe 14: Inrichting van een ondersteunende interne communicatiestructuur

Het gaat hier over de "zenuwbanen" tussen de diverse organisatieonderdelen zoals afdelingen en ook bestuur en RvC. De informatie-eisen moeten aansluiten op ieders verantwoordelijkheden met betrekking tot de interne beheersing. Bij corporaties is privacy en vertrouwelijkheid een punt van extra aandacht. De wijze van communiceren moet in dit kader ook met extra aandacht worden bepaald. (Wat gaat via internet bijvoorbeeld?, Hoe om te gaan met Klantgegevens?

De communicatie moet toegespitst zijn op de doelgroep voor wat betreft tijdigheid. Ook de communicatie over vertrouwelijke informatie moet worden geregeld (geen gebruik van privé mail accounts bijvoorbeeld).

De bestuurder stelt een intern communicatie jaarplan op en legt deze ter goedkeuring aan de RvC voor.

Principe 15: Inrichting van een externe communicatiestructuur

De corporatie heeft veel stakeholders. Daarom is het belangrijk aandacht te hebben voor de externe communicatiestructuur. De corporatie heeft meerdere communicatiekanalen. Denk aan internet, voorlichtingsavonden en interviews in regionale media. De corporatie moet intrinsiek extra aandacht hebben voor de privacy gevoeligheid van de door de corporatie verstrekte informatie.

Corporaties kennen een aantal externe stakeholders die de bedrijfsvoering van de corporatie beoordelen. Denk aan de gemeente, de huurdersorganisatie, het WSW, het ministerie van BZK, Aw en de Visitatiecommissie. Het is verstandig als de bestuurder de informatie en beoordelingen van genoemde partijen aan de RvC voorlegt met zijn visie op de betreffende beoordeling.

De RvC kan zich jaarlijks laten informeren door de bestuurder hoe de corporatie in zijn ogen scoort op de beoordelingspunten van de Aw en het WSW. De RvC vraagt mogelijk de controlfunctie zich hier een oordeel over te vormen en zijn bevindingen te delen met de RvC.

De uitwerking van het MCF op dit principe sluit aan op de governancecode. Deze governancecode kent 5 uitgangspunten waarvan de tweede en de vierde als volgt luiden:

Uitgangspunt 2 Governancecode: "Bestuur en RvC zijn aanspreekbaar en leggen actief verantwoording af Het bestuur is aanspreekbaar op en legt verantwoording af over de maatschappelijke en financiële prestaties van de woningcorporatie als geheel, alsmede over de gemaakte strategische keuzes. De RvC is aanspreekbaar op en legt verantwoording af over het gehouden toezicht".

Uitgangspunt 4 Governancecode: "Bestuur en RvC gaan in dialoog met belanghebbende partijen. De maatschappelijke doelen van de corporatie worden in samenspraak met primair (vertegenwoordigers van) bewoners, en secundair de gemeenten, vastgesteld en neergelegd in prestatieafspraken. Daarnaast hebben corporaties oog voor andere belanghebbende partijen en staan open voor feedback en discussie over de keuzes die zij maken over de inzet van maatschappelijke middelen".

3.5. Monitoring activiteiten: 2 principes (16 t/m 17)

Monitoring is bedoeld om vast te stellen dat het geheel van interne beheersingsmaatregelen nog steeds adequaat werkt conform de bedoeling. De component Monitoring activiteiten is door COSO in 2 principes verder uitgewerkt:

1) inrichten en uitvoeren van continue of periodieke evaluatie van het bestaan en de werking van de interne beheersingsmaatregelen.
2) Tekortkomingen in de interne beheersing worden tijdig gerapporteerd aan partijen die verantwoordelijk zijn voor correctieve maatregelen.

Principe 16: Inrichten en uitvoeren van continue of periodieke evaluatie van het bestaan en de werking van de interne beheersingsmaatregelen

Het is de bedoeling dat de bestuurder periodiek informatie krijgt over de werking van de interne beheersingsmaatregelen. Dit is een taak die normaliter kan worden neergelegd bij de controlfunctie van de corporatie. Deze evaluatie kan worden beoordeeld door de bestuurder en de RvC. Specifiek aandacht wordt besteed aan de vraag of en welke informatie overbodig is. Overbodige informatie kost immers geld en vertroebelt het zicht op wat echt belangrijk is.

Principe 17: Tekortkomingen in de interne beheersing worden tijdig gerapporteerd aan partijen die verantwoordelijk zijn voor correctieve maatregelen

De resultaten van de monitoring activiteiten alsmede de genomen maatregelen kunnen worden vastgelegd en gerapporteerd aan de bestuurder en de RvC. De voortgang van de te nemen maatregelen wordt bewaakt. Het gaat bij de monitoring activiteiten in eerste instantie om de gesignaleerde onvolkomenheden. In tweede instantie gaat het vooral om de vraag waarom de alsnog gesignaleerde onvolkomenheden niet in een eerder stadium door de corporatie zijn ontdekt.

De RvC draagt een grote verantwoordelijkheid voor het toezicht. Deze verantwoordelijkheid kan worden gedragen doordat de RvC expliciet en zichtbaar toezicht houdt op de interne beheersing en vooral op de signalen die uit het interne beheersingssysteem komen. De rapportages van de controlfunctie moeten daarom een prominente plaats op en in de agenda van de RvC hebben. De bevindingen van de controlfunctie zijn relevant op zichzelf, maar de RvC moet samen met de controlfunctie en de bestuurder deze bevindingen vertalen naar gevolgen voor het intern beheersingssysteem.

Bijlage 1. Overzicht van de componenten, de principes en de attributen.