GRC-REGLEMENT

R&A

Woningstichting Eigen Haard

November 2017

Inleiding

Dit GRC-reglement geeft inzicht hoe Eigen Haard uitvoering geeft aan de de belangrijkste grondbeginselen van de GRC-functie binnen de Woningstichting Eigen Haard zoals beschreven in artikel 2.4 van het financieel reglement van de corporatie. Het beschrijft de principes, positionering en bevoegdheden van het bedrijfsonderdeel Risicocontrol & Audit (R&A) op het gebied van Governance, Risk en Compliance (GRC). Hiermee worden de doelstellingen, taken en verantwoordelijkheden verbonden aan de functie, geformaliseerd.

Het doel van de GRC-functie is te voorzien in onafhankelijke en objectieve beoordelingen en adviesdiensten op het gebied van de processen van risicomanagement, interne beheersing en governance op financieel, operationeel en ICT-gebied. Dit zowel op strategisch, tactisch en operationeel niveau. De GRC-functie ondersteunt de organisatie bij het uitvoering geven aan hun verantwoordelijkheden door hen te voorzien van analyses, evaluaties, aanbevelingen op GRC-gebied. De GRC-functie helpt Eigen Haard haar doelstellingen te realiseren door met een systematische, gedisciplineerde aanpak de effectiviteit van risicomanagement, beheersings- en besturingsprocessen te evalueren en te verbeteren.

Positionering van de GRC-functie binnen Eigen Haard

Eigen Haard heeft er voor gekozen de verschillende risico- en controlfuncties te laten samenwerken en op deze manier een geïntegreerde aanpak voor GRC neer te zetten. Dit met als doel om op efficiënte wijze inzicht te krijgen in de belangrijkste risico’s, de beheersing daarvan en een heldere en duidelijke rapportage hierover. R&A rapporteert hiërarchisch aan het voltallige bestuur. Binnen R&A is de GRC-functie vorm gegeven met de benoeming van een aantal (senior) adviseurs risico- en procescontrol met elk een eigen specialisatie op het gebied van auditing, compliance, risicomanagement en procesmanagement.

De onafhankelijkheid van de interne audit wordt gewaarborgd door de verantwoordelijkheid van het auditplan en de uitvoering hiervan te beleggen bij een hierin gespecialiseerd senior auditor. Deze functie is de enige die audits binnen Eigen Haard zal uitvoeren of anderen kan opdragen die uit te voeren. R&A heeft de coördinatie en de regie over alle GRC-gerelateerde audits die door zowel internen als externen binnen Eigen Haard worden uitgevoerd. De manager R&A ontvangt een kopie van elk auditrapport dat door derden is uitgevoerd binnen Eigen Haard.

Verantwoordelijkheden, taken en bevoegdheden

Verantwoordelijkheden

Voor alle medewerkers van het bedrijfsonderdeel R&A geldt dat zij:

- een **proactieve** en **vernieuwende bijdrage** leveren in het realiseren van de strategische doelstellingen door een sleutelrol te vervullen bij de besturing en bedrijfsvoering van Eigen Haard, door zich op te stellen als een **positief kritische business partner** voor de gehele organisatie
- risico's binnen de business signaleren, analyseren en monitoren
- het bestuur, de directie en het management van Eigen Haard bijstaan in het implementeren van de beheersmaatregelen en het uitvoeren van hun verantwoordelijkheden
- afdelingen en medewerkers van Eigen Haard adviseren met betrekking tot hun verplichtingen op het gebied van GRC

Daarnaast draagt R&A zorg voor een eenduidig GRC-beleid dat de basis vormt om medewerkers te adviseren bij het standaardiseren van processen en het integreren van technologie zodat GRC op elk organisatieniveau verankerd is.

Taken en reikwijdte

Het uitgangspunt binnen Eigen Haard is dat het lijnmanagement zelf verantwoordelijk is voor de uitvoering van het GRC-beleid en het beheersen van de risico's. Vanuit de geïntegreerde GRC-functie heeft R&A een signalerende, adviserende en monitorende rol.

<u>Signaleren (risicomitigering / interne audits)</u>

- beoordelen van de toereikendheid en doeltreffendheid van controls op het gebied van risicomanagement, interne beheersing, compliance en governance
- beoordelen van bestaande systemen, beleid, en procedures om vast te stellen dat zij toereikend zijn om ervoor te zorgen dat de onderneming voldoet aan wet- en regelgeving
- beoordelen van audits op ICT-processen en beoordelen van belangrijke systemen na implementatie, om vast te stellen of deze systemen aan de doelen en verwachtingen voldoen en op tijd en binnen budget zijn opgeleverd

<u>Adviseren</u>

- geven van gevraagd en ongevraagd advies met betrekking tot in- en externe ontwikkelingen in de ruimste zin van het woord
- vaststellen dat er passende procedures bestaan binnen de operationele activiteiten voor control self assesments en voortdurende verbetering (borging plan, do, check, act cyclus)
- uitvoeren van specifieke onderzoeken op verzoek van bestuur, directie of de Raad van Commissarissen
- het uitvoeren van analyses op bedrijfskritische processen. Deze analyse kan betrekking hebben op de volgende onderdelen:
    - organisatorische veranderingen
    - standaardisatie van processen ten behoeve van efficiëntie en/of prestatiemanagement
    - risico's en beheersmaatregelen op strategisch, tactisch en operationeel niveau
    - interne beheersing

Monitoren

- monitoren van en rapporteren over incidenten op het gebied van GRC
- adviseren over te nemen beheersmaatregelen om herhaling van incidenten met een zelfde karakter te voorkomen
- monitoren van de opvolging van bevindingen van alle interne en externe audits die van belang zijn voor de GRC-functie

Rapporteren

- rapporteren omtrent de voortgang van geconstateerde bevindingen vanuit interne en externe audits op het gebied van GRC

Bevoegdheden

De medewerkers van R&A hebben in het kader van de uitvoering van hun functie de volgende bevoegdheden:

- uitvoeren van audits en implementeren van control self assessments
- volledige en onbeperkte toegang tot alle informatie van Woningstichting Eigen Haard en de deelnemingen ervan (voor zover dit is toegestaan conform de wet bescherming persoonsgegevens en de algemene verordening gegevensverwerking)
- de mogelijkheid tot het bijwonen van ieder overleg voor zover dit relevant is voor het uitoefenen van de GRC-functie
- directe toegang tot het bestuur, de directie en het management van de divisies
- de mogelijkheid om via de manager R&A te escaleren naar de voorzitter van de Audit Commissie
- verkrijgen van medewerking van iedere individuele medewerker bij de uitoefening van de GRC-functie
- geven van gevraagd en ongevraagd advies over onderwerpen die relevant zijn voor GRC
- initiëren van bijzonder onderzoek na afstemming met het bestuur

De R&A-medewerkers zullen documenten en informatie die aan hen worden verstrekt zorgvuldig behandelen en de vertrouwelijkheid daarvan niet schaden.

Vakbekwaamheid

De manager en medewerkers van R&A dienen de benodigde kennis, vaardigheden en competenties te bezitten die benodigd zijn voor hun individuele verantwoordelijkheden. De formatie als collectiviteit moet voldoende kennis en ervaring op het gebied van risicomanagement, interne beheersing, compliance en governance vergaren en behouden om de verantwoordelijkheid te kunnen dragen.

De manager R&A dient vakkundig advies en ondersteuning te verkrijgen indien de individuele medewerkers van R&A niet de kennis, vaardigheden of competenties hebben om een opdracht geheel of gedeeltelijk uit te voeren. De Raad van Bestuur stelt de manager R&A hiertoe voldoende middelen ter beschikking.

Internal auditing

Relatie met de externe accountant

De relatie tussen R&A en de externe accountant wordt het best beschreven in termen van meewerken en samenwerken. Deze relatie is noodzakelijk door het verschil in doelstellingen. De coördinatie van signaleringsactiviteiten (auditactiviteiten) met de externe accountant bestaat voornamelijk uit het wederzijds informeren en samenwerken om ervoor te zorgen dat:

- de optimale auditdekking wordt bereikt
- er uitwisseling van informatie plaatsvindt
- er minimale duplicering van inzet en kosten is
- er kostenbesparend gebruik wordt gemaakt van het werk van de GRC-adviseurs en de auditor van Eigen Haard

Er is directe en doorlopende communicatie tussen R&A en de externe accountant om de coördinatie van werkzaamheden te bevorderen. Er worden jaarlijks bijeenkomsten met de manager R&A en de externe accountants gehouden, om gebieden vast te stellen waar op elkaars werk kan worden gesteund, of waar het delen van gezamenlijke doelstellingen mogelijk is.

R&A gebruikt de management letter van de externe accountant bij de jaarlijkse risicoanalyse voor het auditplan, ter voorbereiding van een audit en als een voorlopig referentiekader.

Verantwoordingsplicht betreffende rapportages en opvolging bevindingen

De relevante uitkomsten van elke audit, zowel intern als extern uitgevoerd, worden besproken met de proceseigenaar. Na de afronding van elk formeel advies en elke audit wordt door R&A een auditrapport opgesteld. Dit rapport wordt besproken met de proceseigenaar en eventueel procesbeheerder. De proceseigenaar heeft de mogelijkheid om een managementreactie toe te voegen aan het auditrapport. Het auditrapport voorzien van de managementreactie wordt vervolgens besproken met de portefeuillehouder en wordt vervolgens ingebracht in het bestuurlijk beraad. Het auditrapport wordt ter kennisgeving in het directie beraad gebracht.

De proceseigenaar is verantwoordelijk voor de tijdige implementatie van verbeteracties en bevindingen die door de GRC-functie zijn gerapporteerd. Indien van toepassing zal een tijdsduur voor de afronding van de verbeteracties worden opgenomen. Daarnaast houdt hij R&A op de hoogte van de status. Bij vertraging, moet R&A hiervan onderbouwd op de hoogte worden gesteld.

De volgorde en distributie van auditrapportages is als volgt:

	Onderdeel	Distributie aan
1	Auditrapport 0.1	Manager R&A
2	Auditrapport 0.2	Proceseigenaar
3	Auditrapport definitief	Manager R&A Proceseigenaar
4	Managementreactie proceseigenaar	Auditteam
5	Auditrapport 1.0 (is definitief incl. managementreactie)	Bestuur
6	Auditrapport 1.0	Directie Beraad

Jaarcyclus internal auditplan

De jaarcyclus van het auditplan ziet er als volgt uit:

- R&A stelt tenminste eenmaal per jaar (november) het internal auditplan op.
- Het internal auditplan is ontwikkeld op basis van een prioriteitenstelling op basis van het risicomanagementsysteem.
- Bestuur, directie en de Raad van Commissarissen (AuditCie) kunnen input leveren voor het internal auditplan.
- R&A overlegt met de externe accountant over het jaarlijkse internal auditplan.
- Het hieruit resulterende auditplan wordt ter vaststelling voorgelegd aan het bestuur.
- Het door het bestuur vastgestelde auditplan wordt ter goedkeuring voorgelegd aan de Raad van Commissarissen (AuditCie).
- Elke belangrijke afwijking van het goedgekeurde plan zal met het bestuur worden besproken.
- R&A rapporteert periodiek over de auditbevindingen en de status van verbeteracties aan het bestuur en de Raad van Commissarissen middels de Q-rapportage.
- Een jaarlijkse samenvatting van alle auditresultaten wordt aan het bestuur verstrekt, waarbij de Raad van Commissarisen (AuditCie) een afschrift krijgt.
- Bij majeure incidenten is de manager R&A bevoegd direct te rapporteren aan de voorzitter van de Audit Commissie van de Raad van Commissarissen.
- Minimaal eens in de drie jaar evalueert R&A het GRC-reglement, maakt aanpassingen waar nodig en dient deze ter goedkeuring in bij het bestuur en de Raad van Commissarissen (AuditCie).