# Reglement Governance, Risk en Compliance (GRC)

## Woningstichting Eigen Haard

Goedgekeurd door de Raad van Commissarissen op 3 oktober 2024
Vastgesteld door het bestuur op 27 juli 2024

**Inhoudsopgave**

**Inleiding**
Dit reglement geeft inzicht in hoe Eigen Haard, hierna te noemen de Stichting, uitvoering geeft aan de belangrijkste grondbeginselen op het gebied van Governance Risk en Compliance (GRC). Het vormt de verbijzondering van de controlfunctie als bedoeld in het Reglement financieel beleid en beheer van de Stichting.

De Stichting heeft ervoor gekozen de onafhankelijke controlfunctie in een afzonderlijke organisatie-eenheid op te nemen, de afdeling Risicocontrol & Audit. Dit reglement beschrijft dan ook de principes, positionering en bevoegdheden van het bedrijfsonderdeel Risicocontrol & Audit (R&A).

**Doelstelling van de GRC-functie**
Met de invulling van de GRC-functie door de afdeling R&A beoogt de Stichting een proactieve bijdrage te leveren aan de realisatie van de strategische doelstellingen. Dit door de organisatie te voorzien in onafhankelijke en objectieve beoordelingen en adviesdiensten op het gebied van risicomanagement, interne beheersing en governance op zowel strategisch, tactisch als operationeel niveau. Hiermee geeft de afdeling R&A additionele zekerheid inzake naleving van wet- en regelgeving en de juiste werking van processen en mate van risicobeheersing. Ook draagt de afdeling bij aan een adequate besluitvorming door het zijn van een kritische sparringpartner van bestuur, directie en management van de Stichting en hen daar waar nodig te voorzien van tegenspraak.

**Positionering, verantwoordelijkheden en inrichting**

***Positionering***
De Stichting heeft ervoor gekozen de verschillende risico- en controlfuncties te laten samenwerken en op deze manier een geïntegreerde aanpak voor risicocontrol neer te zetten. De afdeling R&A is een afzonderlijke organisatie-eenheid die rechtstreeks onder het bestuur is geplaatst.

De controlfunctie, conform BTiV artikel 105 lid 1 sub e. 4°, wordt uitgevoerd door de manager R&A. De manager R&A kan zowel gevraagd als ongevraagd het bestuur en de RvC adviseren en escaleren naar de Auditcommissie van de RvC. De manager R&A heeft tenminste jaarlijks een gesprek met de voorzitter van de Auditcommissie.

***Three Lines***
Uitgangspunt voor de werking van het GRC binnen de Stichting is het Three Lines model van het IIA (zie ook bijlage 1).

*Eerste lijn*
Het management (directie en staf) van de Stichting is primair verantwoordelijk voor het leveren van producten en diensten aan (interne) klanten en is eerstelijns verantwoordelijkheid voor risicomanagement:

- Geeft leiding en sturing aan acties (inclusief risicomanagement) en de inzet van middelen om de doelstellingen van de Stichting te realiseren.
- Blijft in dialoog met het bestuur en rapporteert over geplande, werkelijke en verwachte resultaten en risico's die gekoppeld zijn aan de doelstellingen.
- Ontwikkelt passende structuren en processen voor de beheersing van activiteiten en risico's (inclusief interne beheersing).
- Draagt zorg voor de daadwerkelijke beheersing van de risico's.
- Draagt zorg voor compliance op het gebied van wet- en regelgeving en ethiek.

*Tweede lijn*
Zowel binnen het management als binnen de afdeling R&A wordt invulling gegeven aan de tweedelijnsrol op het gebied van risicomanagement. De tweedelijns rol van signaleren, informeren, faciliteren, adviseren en monitoren ten aanzien van compliance is belegd bij de afdeling Juridische Zaken. De tweedelijnsrol voorziet in aanvullende expertise, ondersteuning, monitoring en een kritische blik met betrekking tot risicomanagement, waaronder:

- De ontwikkeling, implementatie en voortdurende verbetering van risicomanagement[1] op het strategisch, tactisch en operationeel niveau.
- Het realiseren van doelstellingen voor risicomanagement zoals o.a. naleving van wet- en regelgeving, aanvaardbaar ethisch gedrag; interne beheersing etc.

Daarnaast verstrekt de tweedelijnsrol analyses en rapporteert over de toereikendheid en effectiviteit van risicomanagement. De primaire verantwoordelijkheid hiervoor is belegd bij R&A. Uitzondering hierop is Financial en Business & Projectcontrol. De verantwoordelijkheid hiervoor is belegd bij de divisie Finance & Control. Deze verantwoordelijkheden zijn specifiek beschreven in het Reglement financieel beleid en beheer.

De manager R&A is het Meldpunt voor mogelijke misstanden en het melden bij vermoeden van onregelmatigheden of integriteitsincidenten. De kaders zijn opgenomen in de Meldregeling als bedoeld in de Wet bescherming klokkenluiders (Wbk).

*Derde lijn*
De derdelijn betreft de interne auditrol en is belegd bij de afdeling R&A. Kenmerkend voor deze rol is de onafhankelijkheid ten opzichte van het management. Door het uitvoeren van interne audits voorziet R&A in aanvullende, onafhankelijke en objectieve assurance met betrekking tot de toereikendheid en effectiviteit van governance en risicomanagement. Naast het bieden van zekerheid hebben deze audits als doel om continue verbetering van processen te bevorderen.

***Formatie en vakbekwaamheid***
Het bestuur stelt de manager R&A voldoende capaciteit en middelen beschikbaar voor de uitvoering van haar werkzaamheden. De manager R&A beschikt over een aantal (senior) adviseurs om de primaire taken op het gebied van risicomanagement en auditing te kunnen uitvoeren. Op onderdelen wordt samengewerkt met deskundige externe partijen op het gebied van GRC. Door te participeren in een compliance team met de afdeling Juridische Zaken draagt de R&A bij aan de monitoring en beheersing van compliance risico's.

De manager R&A ziet erop toe dat de formatie als collectiviteit over voldoende capaciteit, kennis en ervaring, vaardigheden en competenties beschikt om de verantwoordelijkheid te kunnen dragen.

**Taken en bevoegdheden**

***Taken***
Vanuit de geïntegreerde GRC-functie vervult de afdeling R&A zowel tweede- als derdelijnstaken.
Specifiek voor de invulling van risicomanagement:
- Initiëren, bewustmaken en ondersteunen van de ontwikkeling, implementatie en voortdurende verbetering van risicomanagement op strategisch, tactisch en operationeel niveau.
- Beoordelen en uitvoeren van analyses op de toereikendheid en doeltreffendheid van controls op het gebied van risicomanagement en interne beheersing.
- Beoordelen en uitvoeren van analyses op systemen, beleid en procedures om vast te stellen of zij toereikend zijn om ervoor te zorgen dat de onderneming voldoet aan wet- en regelgeving.
- Gevraagd en ongevraagd signaleren van en adviseren over risico's met betrekking tot in- en externe ontwikkelingen in de ruimste zin van het woord.
- Meedenken en adviseren over relevante besluitvorming als proactief kritische sparringspartner van bestuur, directie en management.
    - In de statuten van de stichting en het reglement van het bestuur is een aantal bestuursbesluiten specifiek benoemd dat goedkeuring behoeft van de RvC. Tenminste bij deze besluiten zal de financiële en controlfunctie (directeur F&C en manager R&A) worden betrokken.
- Adviseren van bestuur, directie en het management over beheersing en hen ondersteunen bij de implementatie van de beheersmaatregelen.
- Zorgdragen dat het procuratiereglement minimaal een keer in het jaar is geactualiseerd.

[1] *Gezien de scope en werking van integraal risicomanagement is dit werkgebied nader uitgewerkt en te lezen in het Risicomanagementbeleid*

- Uitvoeren van specifieke onderzoeken op verzoek van bestuur, directie of de RvC.
- Integraal rapporteren aan bestuur, directie en management van geconstateerde bevindingen en de opvolging hiervan (GRC tertaalrapportage). Deze rapportage wordt geagendeerd in de auditcommissie.

Specifiek voor de invulling van internal auditing:
- R&A stelt jaarlijks (november) het intern auditplan op met daarin de voor dat jaar te auditen processen
    - Het intern auditplan is gebaseerd op:
        - het onderliggende auditlandschap (proceslandschap van de Stichting en materialiteit van de processen);
        - de strategische risicoanalyse;
        - bevindingen vanuit voorgaande audits en managementletter punten;
        - de verdeling over de divisies;
        - Input van RvC, bestuur, directie en management.
    - R&A overlegt regelmatig met de externe accountant over het jaarlijkse intern auditplan en de resultaten zodat de optimale auditdekking wordt bereikt en er uitwisseling van informatie plaatsvindt.
    - Het intern auditplan wordt vastgesteld door het bestuur en vervolgens ter goedkeuring voorgelegd aan de auditcommissie van de RvC.
    - Elke belangrijke afwijking van het goedgekeurde plan zal met het bestuur worden besproken.
- Adviseurs van de afdeling R&A voeren de audits uit of laten onder regie de audits uitvoeren door een externe auditor.
    - Om de onafhankelijkheid te waarborgen wordt een audit niet geleid door een adviseur die het dagelijks contact met de proceseigenaar onderhoudt of over het te auditen onderwerp recent heeft geadviseerd.
    - De audits op processen waarvan R&A eigenaar is, worden zo nodig uitgevoerd door een externe auditor.
- R&A stemt de specifieke scope van elke afzonderlijke audit af met het bestuur en de proceseigenaar.
- R&A stelt de proceseigenaar op basis van het definitieve concept auditrapport in de gelegenheid om een managementreactie toe te voegen. Deze managementreactie wordt integraal opgenomen in het rapport. Na toevoeging van de managementreactie is het auditrapport definitief.
- Het bestuur bespreekt de definitieve auditrapportage en stuurt deze ter informatie aan het directieberaad.
- R&A rapporteert periodiek over de auditbevindingen en de status van verbeteracties aan het bestuur en directieberaad in haar GRC tertaalrapportage. Deze rapportage wordt geagendeerd in de auditcommissie.
- Manager R&A is bevoegd direct te rapporteren aan de voorzitter van de auditcommissie van de RvC bij majeure incidenten.
- Manager R&A rapporteert aantasting van onafhankelijkheid en objectiviteit bij de invulling van haar rol aan het bestuur, met een escalatiemogelijk naar de voorzitter van de auditcommissie van de RvC.

Voor alle (senior) adviseurs van de afdeling R&A geldt dat zij:
- Een proactieve en vernieuwende bijdrage leveren in het realiseren van de strategische doelstellingen bij de besturing en bedrijfsvoering van de Stichting.
- Documenten en informatie die aan hen worden verstrekt zorgvuldig behandelen en de vertrouwelijkheid ervan niet schaden.
- Zich onafhankelijk, objectief en als positief kritische business partner voor de gehele organisatie opstellen.
- Over een analytisch denkvermogen en professionele communicatievaardigheden beschikken en zich blijven bijscholen in voor de uitoefening van hun functie relevante onderwerpen en gebieden.

***Bevoegdheden***
De afdeling R&A heeft in het kader van de uitvoering van haar functie de volgende bevoegdheden:

- Volledige en onbeperkte toegang tot alle informatie van de Stichting en de deelnemingen ervan.
- 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, RvC, de directie en het management van de divisies en staf.
- 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.
- Uitvoeren van audits conform het auditplan.
- Initiëren van bijzonder onderzoek na afstemming met het bestuur.
- Regie en coördinatie over alle GRC-gerelateerde audits die door zowel internen als externen binnen de Stichting worden uitgevoerd. De manager R&A ontvangt een kopie van elk auditrapport dat door derden is uitgevoerd binnen de Stichting.
- De mogelijkheid om via de manager R&A te escaleren naar de voorzitter van de auditcommissie van de RvC.

**Evaluatie en aansturing**
Dit GRC-reglement wordt tenminste 3-jaarlijks geëvalueerd door R&A en vastgesteld door het bestuur, na de voorafgaande goedkeuring van de RvC.

**Bijlage 1: Organisatie inrichting**
Eigen Haard is in overeenstemming met de eisen van toezichthouders ingericht en baseert zich daarbij op het 'Three Lines Model' (IIA 2020).