Charter Internal Audit

2022

Colofon

Titel	Charter Internal Audit
Datum	02/12/2021
Status	Definitief
Gericht aan	Raad van Bestuur Audit & Compliance Committee (van de Raad van Toezicht)
Auteur	Michel Vlak Manager Internal Audit

Inhoudsopgave

1 Inleiding

Erasmus MC heeft een eigen statutaire Raad van Bestuur en Audit & Compliance Committee (onderdeel van de Raad van Toezicht). De Manager Internal Audit rapporteert hiërarchisch aan de CFO en functioneel aan de voorzitter van het Audit & Compliance Committee (ACC).

Het Charter Internal Audit is bedoeld om de functie van Internal Audit binnen het Erasmus MC nader te definiëren en haar positie en autoriteit transparant weer te geven. Internal Audit voldoet met dit Charter aan de eisen van het Institute van Internal Auditors.

2 Missie

Het Institute van Internal Auditors hanteert de volgende definitie van Internal Auditing:
"Internal auditing biedt onafhankelijke en objectieve assurance- en adviesdiensten, die bedoeld zijn om meerwaarde te leveren en de activiteiten van een organisatie te verbeteren. De internal auditfunctie helpt een organisatie haar doelstellingen te realiseren door op basis van een systematische en gedisciplineerde aanpak de effectiviteit van de processen van governance, risicomanagement en beheersing te evalueren en te verbeteren" (IIA Inc).

Deze definitie vormt het richtsnoer voor de inrichting en werkzaamheden van Internal Audit. De missie van Internal Audit is om Erasmus MC te ondersteunen bij het bereiken van haar doelstellingen, door het zorgvuldig, deskundig, kritisch en objectief beoordelen van de governance, beheersingsmaatregelen, risicomanagement en integriteit en daarover gevraagd of ongevraagd te adviseren.

3 Taakopdracht Internal Audit

3.1 Algemeen

Internal Audit is een permanente, onafhankelijke functie die aanvullende zekerheid verschaft aan de Raad van Bestuur en de Raad van Toezicht over de beheersing, effectiviteit en het compliant zijn van de bedrijfsvoering. Zij rapporteert en adviseert gevraagd en ongevraagd ten aanzien van gesignaleerde verbeterpunten in het governance-, risicomanagement-, integriteit- en beheersingsraamwerk. Internal Audit verstrekt geen accountantsverklaringen of assurance rapportages met externe werking (niet wettelijk voorgeschreven).

Om invulling te geven aan haar taakopdracht beoordeelt Internal Audit op een gestructureerde wijze de kwaliteit en effectiviteit van interne beheersing van het Erasmus MC. Internal Audit draagt hierdoor bij aan de verbetering van de bedrijfsvoering en het bereiken van de doelstellingen van het Erasmus MC.

De beoordeling door Internal Audit richt zich, tegen de achtergrond van het risicoprofiel en de risicobereidheid (risk appetite), met name op:

- governance, cultuur, verdeling van taken, verantwoordelijkheden en bevoegdheden;
- beheersing van processen op het gebied van bedrijfsvoering, zorg, onderzoek en onderwijs inclusief de naleving van beleidskaders, procedures en protocollen:
- betrouwbaarheid van gegevensverwerkende processen (IT en administratieve systemen) en relevante (financiële) stuur- en verantwoordingsinformatie;
- naleving van externe wet- en regelgeving, inclusief het functioneren van 2e lijnsfuncties;
- bescherming van middelen (gebouwen, medische technologie, financiële middelen en personeel).

3.2 Audits

Internal Audit is primair gericht op het geven van een redelijke mate van zekerheid over of inzicht in de kwaliteit van de interne beheersing (assurance). Daarbij voert zij onderstaande werkzaamheden uit, voor zover voldoende kennis, vaardigheden of competenties aanwezig zijn binnen de afdeling:

- *Operational audits:* gestructureerde onderzoeken gericht op de kwaliteit van de proces- en risicobeheersing, risicomanagement en besturing (governance). Hierbij wordt afhankelijk van de stelling opzet, bestaan en/of werking van de interne (risico)beheersing onderzocht.
- *IT audits*: gericht op het beoordelen van de kwaliteit van de IT Governance, operationele ICT-systemen, technische infrastructuur, informatiebeveiliging en technologische ontwikkelingen.
- *Compliance audits*: gericht op het beoordelen en toetsen van de implementatie en naleving van wet- en regelgeving, procedures en richtlijnen.
- *Programma en project audits*: gericht op het beoordelen van de kwaliteit van de beheersing van risico's binnen de kritische programma's en projecten van Erasmus MC.
- *Financial audits*: gericht op de betrouwbaarheid van de externe verantwoordingsinformatie, zoals jaarrekening, subsidieverantwoordingen en horizontaal toezicht. Deze werkzaamheden worden uitgevoerd ten behoeve van de externe accountant of zorgverzekeraars, waarbij gesteund wordt op Internal Audit.
- *Fraude onderzoeken*: werkzaamheden met een verifiërend karakter, bestaande uit het verzamelen en analyseren van al dan niet financiële gegevens en het rapporteren van de uitkomsten, gericht op het functioneren, handelen of nalaten van handelen van een betrokkene, te weten een (rechts)persoon.
- *Review/Quick Scan:* onderzoeken met minder diepgang en lagere mate van zekerheid.
- *Inventarisatie/beschrijvend onderzoek*: gericht op het in kaart brengen c.q. inzichtelijk maken van een specifiek onderwerp of beheersingsvraagstuk.

3.3 Advies

Internal Audit kan worden gevraagd te adviseren bij de inrichting van de governance, risicobeheersing of implementatie van wet- en regelgeving of over mogelijke verbeteringen van de AO/IC. Dergelijke advies-opdrachten worden zorgvuldig beoordeeld, waarbij Internal Audit ervoor dient te waken dat zij haar onafhankelijke positie niet verliest of management verantwoordelijkheid neemt. Naast adviesopdrachten, betreft advisering vanuit Internal Audit ook activiteiten op het gebied van spiegelen, coaching, faciliteren, opleiden van medewerkers in de organisatie en bijdragen aan werkgroepen, vanuit het perspectief van interne beheersing en/of vaktechniek (audit- en controletechnieken).

4 Onafhankelijkheid en objectiviteit

Internal Audit is een permanente, onafhankelijke functie binnen het Erasmus MC. Haar medewerkers zijn objectief bij de uitvoering van hun werkzaamheden. Internal Audit is vrij om al haar bevindingen en beoordelingen zonder vooroordelen en interventie te rapporteren. De onafhankelijkheid is gewaarborgd doordat Internal Audit rechtstreeks rapporteert aan de CFO en een directe communicatielijn heeft met de voorzitter van het Audit & Compliance Committee. Daarnaast heeft Manager Internal Audit, indien deze dit noodzakelijk acht, rechtstreeks toegang tot de voorzitter van de Raad van Bestuur en de voorzitter van het Audit & Compliance Committee.

4.1 Onafhankelijkheid

De Manager Internal Audit wordt benoemd, ontslagen en beoordeeld door de Raad van Bestuur. Het Audit & Compliance Committee is inhoudelijk betrokken, heeft inspraak en geeft goedkeuring aan de benoeming of het ontslag van de Manager Internal Audit en geeft input voor en goedkeuring aan de jaarlijkse beoordeling.

Als onderdeel van haar verantwoordelijkheid treft de Raad van Bestuur alle noodzakelijke maatregelen, die waarborgen dat de organisatie voortdurend kan vertrouwen op een adequaat functionerende auditfunctie. Het Audit & Compliance Committee houdt in haar functie toezicht op de Raad van Bestuur ten aanzien van de rol, het onafhankelijk functioneren en de bezetting van Internal Audit. Daarnaast is de Manager Internal Audit gemachtigd om direct contact op te nemen met de voorzitter van het Audit & Compliance Committee indien de situatie daartoe aanleiding geeft.

4.2 Objectiviteit

Internal Audit staat los van de (dagelijkse) beheersingsmaatregelen in de diverse bedrijfsprocessen. Internal Audit draagt geen management verantwoordelijkheid en is niet betrokken bij het implementeren van maatregelen met betrekking tot risicomanagement, compliance en interne beheersing. Medewerkers van Internal Audit, die geworven worden binnen Erasmus MC, zullen het eerste jaar geen controle- en/of advieswerkzaamheden uitvoeren in de bedrijfsonderdelen waar zij in hun vorige functie nauw bij betrokken zijn geweest.

5 Scope, bevoegdheid en verantwoordelijkheid

5.1 Scope en planning

De scope van Internal Audit omvat alle afdelingen, processen (inclusief uitbestede processen), systemen en functies die onder de verantwoordelijkheid vallen van het Erasmus MC. Het lijnmanagement is verantwoordelijk voor ontwerp en implementatie van het interne beheersing- en het risicomanagement framework binnen de bedrijfsprocessen en wordt daarbij ondersteund door (de)centrale afdelingen binnen de organisatie.

Internal Audit stelt jaarlijks een audit jaarplan op. De selectie van onderwerpen voor het audit jaarplan is gebaseerd op een jaarlijks (geactualiseerde) risicoanalyse en wordt besproken met en goedgekeurd door de Raad van Bestuur. Het definitieve jaarplan wordt vastgesteld door het Audit & Compliance Committee, met recht tot amendering.

Internal Audit is verantwoordelijk voor de uitvoering van de geplande audits. De Raad van Bestuur, Themadirecteuren en Pijlerdirecteuren houden Internal Audit geïnformeerd over wijzigingen in de governance, nieuwe ontwikkelingen, initiatieven, operationele wijzigingen, gebreken in de interne controle en/of afwijkingen van regels zodat (potentiële) risico's in een vroegtijdig stadium kunnen worden gesignaleerd. Op het moment dat de Raad van Bestuur of directies kennis hebben van (mogelijke) incidenten binnen de bedrijfsvoering van het Erasmus MC, wordt Internal Audit direct en volledig geïnformeerd.

5.2 Bevoegdheden

Internal Audit heeft de bevoegdheid om het audit jaarplan gedurende het jaar aan te passen naar aanleiding van nieuwe inzichten, ontwikkelingen, prioriteiten en managementverzoeken. De wijzigingen worden overlegd met de Raad van Bestuur en goedgekeurd door het Audit & Compliance Committee. Om haar taken zo effectief mogelijk te kunnen is Internal Audit bevoegd om binnen het gehele verantwoordelijkheidsgebied direct kennis te mogen nemen van alle informatie (inclusief notulen van de algemene vergaderingen van de Raad van Bestuur en de Raad van Toezicht) en alle werkzaamheden uit te voeren die naar het inzicht van Internal Audit in dit kader van belang zijn.

5.3 Uitvoeren, rapporteren en verantwoorden

Internal Audit is verantwoordelijk voor het plannen en uitvoeren van de activiteiten die zijn opgenomen in het audit jaarplan, evenals voor het rapporteren van haar bevindingen inzake de kwaliteit van de governance, werking van beheersingsmaatregelen of risicomanagement. Internal Audit bepaalt, in overleg met de opdrachtgever of auditee, de scope van het onderzoek, waarbij de aanpak risicogebaseerd is. Voorafgaand aan een onderzoek

wordt een Plan van Aanpak opgesteld en het normenkader vastgesteld en besproken met de auditee, zodat voor aanvang duidelijk is waarnaar gekeken wordt, hoe het onderzoek wordt uitgevoerd, welke informatiebronnen worden ingezet, waartegen wordt getoetst (toetsingscriteria) en hoe er wordt gerapporteerd.

Ten behoeve van een effectieve uitvoering van opdrachten heeft Internal Audit onbeperkte toegang tot dossiers, personeel en fysieke eigendommen, mits relevant in het kader van de realisatie van de auditdoelstellingen. In het kader van (fraude)onderzoeken heeft Internal Audit mogelijk toegang tot bijzondere persoonsgegevens, waarbij bij het raadplegen en vastleggen de grootste zorgvuldigheid wordt betracht. Uiteraard worden de regels die voortvloeien uit de Algemene Verordening Gegevensbescherming (AVG) nageleefd en wordt waar nodig contact opgenomen met de Functionaris Gegevensbescherming (FG). Bij een verzoek om inzagerecht in een fraudedossier vanuit privacy optiek worden zorgvuldige overwegingen gemaakt, zodat alleen privacy gerelateerde gegevens kunnen worden bekeken conform de bedoeling van de AVG.

Internal Audit rapporteert, na bespreking met het betrokken management en het informeren van het verantwoordelijk RvB lid, de uitkomsten van haar onderzoeken rechtstreeks aan de Raad van Bestuur. Het rapport bevat onder andere de doelstelling en scope van de audit, bevindingen en door actiehouders geformuleerde verbeterplannen. De verantwoordelijkheid voor de implementatie van de verbeterplannen ligt in de lijnorganisatie. Internal Audit bewaakt op kwartaalbasis wel de voortgang en effectiviteit van de verbeterplannen.

De Manager Internal Audit heeft periodiek overleg met de CFO, waarbij de status van het auditplan en onderhanden audits worden besproken evenals relevante onderwerpen en interne en externe ontwikkelingen. Audit rapporten worden besproken in de RvB vergadering, alvorens deze beschikbaar zijn voor het Audit & Compliance Committee.

Periodiek rapporteert Internal Audit aan de Raad van Bestuur over ontwikkelingen en (potentiële) risico's, de belangrijkste bevindingen in de afgelopen periode, de voortgang en effectiviteit van de verbeterplannen voortkomende uit audits, de voortgang van het auditjaarplan en de ontwikkeling van de afdeling (kwaliteitssysteem). Na bespreking in de Raad van Bestuur wordt het rapport besproken in het Audit & Compliance Committee en beschikbaar gesteld voor de Raad van Toezicht.

6 Gedrags- en beroepsregels

Internal Audit is gehouden haar werkzaamheden te verrichten, in overeenstemming met de geldende (gedrags) richtlijnen van het Erasmus MC en algemeen geaccepteerde nationale en internationale professionele standaarden, in het bijzonder de 'Code of Ethics' van IIA, de Gedrags- en beroepsregels Register Operational Auditors' (IIA/SVRO) en de richtlijnen van het NBA (VGBA, ViO, RKB1 en NV COS) en NOREA/ISACA.

Het doel van deze normen is het waarborgen van een goede kwaliteit van de beroepsuitoefening, waaronder:

- bewaking van de onafhankelijkheid en onpartijdigheid.
- waarborging van de geheimhouding.
- waarborging van beroepsmatige deskundigheid en zorgvuldigheid.
- ontwikkeling en bijhouden van essentiële kennis en vaardigheden.

7 Kwaliteitsborging

Internal Audit dient te beschikken over voldoende middelen en medewerkers, zodat zij alle werkzaamheden op verantwoorde en deskundige wijze kan verrichten. De omvang en samenstelling van de formatieplaatsen moet zodanig zijn dat er voldoende toegesneden (ook specialistische) kennis en ervaring aanwezig is, zodat Internal Audit blijvend effectief kan functioneren. Naleving van de gedrags- en beroepsregels brengt met zich mee dat

Internal Audit zorg dient te dragen voor een goede onderbouwing van de rapportages en adequate dossiervastleggingen van de werkzaamheden.

Om aan de beroepsstandaarden te voldoen, is een reeks van maatregelen getroffen. De kernbezetting van Internal Audit bestaat uit gekwalificeerde audit professionals (RA, RO, RE, CISA, CISM en CFE), met meerjarige ervaring in het vakgebied, die lid zijn van een beroepsvereniging (IIA/SVRO, NBA, NOREA, ISACA, ACFE) en. Daarnaast wordt voorzien in educatie.

Internal Audit richt haar processen zodanig in dat doorlopend aan de door de beroepsorganisaties vastgelegde normen en standaarden kan worden voldaan. Daartoe beschikt zij over een kwaliteitssysteem waarmee de kwaliteit van de processen en producten van Internal Audit kan worden gewaarborgd. Dit is vastgelegd in het Handboek Internal Audit.

Het kwaliteitssysteem bestaat uit kwaliteitsbewaking per audit en algemene evaluaties. Deze systematiek bestaat uit interne reviews en continue beoordeling of het kwaliteitssysteem functioneert, met jaarlijkse formele beoordeling door de Manager Internal Audit. Uitkomsten van kwaliteitstoetsingen en evaluaties en verbeteracties worden opgenomen in de periodieke rapportage.

8 Relatie met interne functies

Internal Audit onderscheidt zich van andere interne functies op het gebied van kwaliteit, controle en assurance, zoals de afdelingen Kwaliteit & Patiëntenzorg, Zorgadministratie, Risk & Compliance, CISO en FG, et cetera aangezien het geen beleidsbepalende en/of uitvoerende rol heeft binnen de bestaande systemen van risicomanagement, compliance en interne beheersing.

Dit stelt Internal Audit in staat een objectief oordeel te geven over de opzet en de werking van de governancestructuur, de risicomanagement systemen en de interne beheersing. In dat oordeel betrekt Internal Audit, indien van toepassing, ook het functioneren van deze interne functies. Aard en diepgang van de door Internal Audit uit te voeren werkzaamheden worden daarnaast afgestemd op de werkzaamheden van deze interne functies, zodat doublures en onnodige belasting van de organisatie worden voorkomen en relevantie wordt gewaarborgd.

Internal Audit heeft periodiek overleg met interne functies op het gebied van kwaliteit, controle en assurance, waarbij gesproken wordt over belangrijke ontwikkelingen en risico's en kennis en ervaringen worden gedeeld. Waar mogelijk wordt gezamenlijk opgetrokken bij het uitvoeren van onderzoeken.

9 Relatie met externe instanties

9.1 Externe accountant

De externe accountant, belast met de controle van de te certificeren financiële verantwoordingen, maakt op een aantal onderdelen gebruik van door Internal Audit uitgevoerde werkzaamheden. De externe accountant kan audit rapporten ontvangen, nadat de definitieve rapporten met de Raad van Bestuur zijn besproken en de interne governance hebben doorlopen.

9.2 Zorgverzekeraars

Horizontaal Toezicht richt zich op de rechtmatigheid van de zorguitgaven en is een vorm van samenwerking tussen de zorgverzekeraars en een zorgaanbieder die steunt op vertrouwen, wederzijds begrip en transparantie in

handelen. Internal Audit voert specifieke controlewerkzaamheden uit op verantwoordingen die door de lijnorganisatie worden aangeleverd ten behoeve van verzekeraars.

9.3 Toezichthouders

Toezichthouders, zoals IGJ, kunnen hun toezicht op een directe wijze uitvoeren door bij het Erasmus MC onderzoeken in te stellen. Als onderdeel daarvan kunnen zij ook de mening of rapporten opvragen van Internal Audit over specifieke onderwerpen. Internal Audit stelt op verzoek auditrapportages aan toezichthouders ter beschikking, nadat definitieve rapporten met de Raad van Bestuur zijn besproken en de interne governance hebben doorlopen.

10 Goedkeuring van het Charter

Dit Charter Internal Audit wordt jaarlijks beoordeeld, rekening houdend met interne en externe ontwikkelingen, waarbij mogelijke implicaties voor de governance en het dienstenpakket worden meegenomen. Het Charter Internal Audit wordt goedgekeurd door de Raad van Bestuur en vastgesteld door het Audit & Compliance Committee van het Erasmus MC.

Het Charter Internal Audit 2022 is op 2 december 2021 vastgesteld.