

Actief sturen op doelrealisatie

Kader Risicomanagement HR

2026-2030



**HOGESCHOOL
ROTTERDAM**

Toekomstmakers

DOCUMENTINFORMATIE

Vaststelling

Versie	Datum	Vastgesteld door
1.0	29-09-2026	College van Bestuur

Samenhang met andere documenten

Naam	Bovenliggend	Gelijk	Onderliggend
Kader Bedrijfscontinuïteitsbeheer (BCM)		X	
Crisismanagementplan HR (CMP)		X	
Risk appetite statement HR			X
Informatiebeveiligingsbeleid		X	x

Brondocumenten

Kader
COSO ERM 2017
NEN-ISO 31000 + C11:2019 nl
Charter Risk Manager
Branchecode goed bestuur en toezicht in het hbo (2023)
Handboek kwaliteitszorg Hogeschool Rotterdam (2025)

INHOUDSOPGAVE

Inleiding	5
1. Visie op risicomanagement	5
2. Doel van het kader	6
2.1. Uitgangspunten	6
2.2. Scope	6
3. Definities	7
4. Rollen en verantwoordelijkheden	8
5. Het risicomanagementproces	10
6. Risicohouding en risicobereidheid	11
Referenties	13

Inleiding

De Branchecode Goed bestuur en toezicht van de VH schrijft voor dat we de risico's verbonden aan onze taken kennen en beheersen door middel van een systeem van interne kwaliteitszorg.¹ Hogeschool Rotterdam (HR) opereert in een omgeving waarin maatschappelijke ontwikkelingen, digitalisering, nieuwe wet- en regelgeving en veranderende eisen vanuit ons beroepenveld continu nieuwe kansen en onzekerheden creëren. Het borgen van de continuïteit, kwaliteit en integriteit van ons onderwijs, onderzoek en onze bedrijfsvoering vraagt dan ook om een gestructureerde, transparante en toekomstgerichte aanpak van risicomanagement.

1. Visie op risicomanagement

Risicomanagement binnen Hogeschool Rotterdam staat niet op zichzelf, maar is integraal onderdeel van goed bestuur en professioneel handelen binnen de kaders van het Three Lines Model (3LM). Het ondersteunt continue verbetering volgens de PDCA-cyclus, helpt ons omgaan met onzekerheden en ondersteunt actieve sturing bij het realiseren van onze doelen.

Risicomanagement draagt bij aan de realisatie van de doelen uit onze strategische agenda (SA) en is verankerd in onze vier kernwaarden: **verantwoordelijkheid** voor het tijdig signaleren en afwegen van risico's, **veerkracht** bij het wendbaar inspelen op veranderingen, **verbondenheid** in de gezamenlijke aanpak binnen en buiten de organisatie, en **rechtvaardigheid** in transparante en zorgvuldige afwegingen die passen bij onze maatschappelijke opdracht.

We kennen en beheersen onze risico's via ons systeem van interne kwaliteitszorg, waarin risicomanagement en kwaliteitszorg beide geïntegreerd zijn. De samenhang bestaat eruit dat beide processen gericht zijn op continue verbetering. Kwaliteitszorg richt zich op het verbeteren van de kwaliteit door en van mensen, producten en processen, terwijl risicomanagement gericht is op omgaan met de onzekerheden die op ons pad komen. Door beide processen te integreren, bevorderen we een cultuur van continue verbetering.

Kwaliteitszorg en risicomanagement versterken elkaar. Door risico's en kansen te identificeren die de kwaliteit beïnvloeden kunnen we proactief maatregelen nemen om toekomstbestendig te worden en te blijven. Zo waarborgen we de kwaliteit van onze producten en processen.

Beide processen zijn sterk afhankelijk van gegevens en analyse; kwaliteitszorg vereist het verzamelen en analyseren van gegevens over kwaliteit en het bereiken van doelstellingen, terwijl risicomanagement betrokken is bij het analyseren van gegevens over onzekerheden om potentiële kansen en risico's te identificeren. Het combineren van deze gegevens geeft een holistisch beeld van de huidige staat van de kwaliteit en onze toekomstbestendigheid.²

¹ Branchecode goed bestuur en toezicht in het hbo, 2023

² Kwaliteitshandboek HR, 2026

Onze aanpak van risicomanagement is geïntegreerd in de besturing en kwaliteitszorg, is systematisch en proportioneel, en wordt afgestemd op de context van de hogeschool. We trekken relevante stakeholders erbij te betrekken, maken gebruik van best beschikbare informatie en besteden expliciet aandacht aan mens en cultuur.

2. Doel van het kader

Het kader risicomanagement biedt een hogeschoolbreed, consistent en systematisch uitgangspunt voor het identificeren, analyseren, beoordelen en beheersen van risico's die de realisatie van onze strategische ambities kunnen beïnvloeden. Het ondersteunt de uitvoering van onze strategische agenda en draagt bij aan een sterke, betrouwbare en toekomstbestendige organisatie. Het kader heeft vijf doelen:

1. Bijdragen aan het actief sturen op doelrealisatie
2. Waarborgen van de continuïteit en kwaliteit van onderwijs, onderzoek en bedrijfsvoering door risico's tijdig te herkennen en adequaat te beheersen
3. Borgen van transparante en zorgvuldige besluitvorming
4. Vergroten van aanpassingsvermogen en veerkracht
5. Bevorderen van samenwerking en gedeeld risicobewustzijn

Dit kader is uitdrukkelijk geen separaat document maar dient gelezen te worden in samenhang met hogeschoolbrede kaders op de binnen de hogeschool te onderscheiden beheersgebieden.

2.1. Uitgangspunten

Binnen HR hanteren we integraal risicomanagement: risico's van de verschillende beheersgebieden worden in onderlinge samenhang beoordeeld en gemanaged. Het kader hanteert de volgende uitgangspunten:

1. Risicomanagement maakt onderdeel uit van de PDCA van alle primaire en ondersteunende processen.
2. Risicomanagement is geïntegreerd in de planning- en controlcyclus.
3. Risicobeheersing is proportioneel, doelmatig en passend bij onze risicobereidheid.
4. Risico's worden tijdigesignaleerd en open besproken, in lijn met onze kernwaarden.
5. Risicomanagement is een gezamenlijke opgave, verbondenheid is leidend.
6. De hogeschool ontwikkelt haar aanpak continu, om wendbaarheid te versterken.

2.2. Scope

Dit kader is van toepassing op de gehele populatie binnen de hogeschool en op alle processen en activiteiten. Medewerkers, leidinggevend en bestuurders dragen vanuit hun rol binnen het 3LM bij aan risicobewust en verantwoord handelen binnen hun eigen PDCA.

Dit geldt expliciet ook voor projecten en programma's: bij de start, uitvoering en afsluiting van projecten worden risico's systematisch geïdentificeerd, geanalyseerd en gemonitord, en worden de belangrijkste projectrisico's opgenomen in de risicoprofielen van de betrokken organisatieonderdelen en in het hogeschoolbrede portfoliomanagement. De scope omvat strategische, tactische en operationele risico's, met bijzondere aandacht voor risico's die

samenhangen met de ambities uit de strategische agenda en de vier maatschappelijke opgaven.

3. Definities

Voor dit kader zijn de volgende definities relevant:

Risico:

Effect van onzekerheid op (het behalen van) de doelstellingen van Hogeschool Rotterdam. Dit effect kan zowel positief als negatief zijn.

Gevolg

Uitkomst van een gebeurtenis waardoor doelstellingen worden beïnvloed.

Waarschijnlijkheid

De kans dat een risico zich voordoet. Bij een negatief risico is de waarschijnlijkheid een combinatie van een blootstelling aan een (1) dreiging en het benutten van een (2) kwetsbaarheid:

(1) Dreiging:

Elke externe of interne bron van gevaar die, wanneer zij zich manifesteert, kan leiden tot een ongewenste gebeurtenis met negatieve gevolgen voor de organisatie. Een dreiging is nog geen risico en nog geen incident.

(2) Kwetsbaarheid:

De zwakte die door de dreiging kan worden benut. Het is een mogelijke oorzaak van ongewenste gebeurtenissen.

$$\text{Risico} = (\text{Dreiging} \times \text{Kwetsbaarheid} = \text{Waarschijnlijkheid}) \times \text{Gevolg}$$

Risicohouding:

De cultuur en houding tegenover risico, bepaald door de manier waarop medewerkers en management risico's en kansen waarnemen, bespreken en behandelen, en de mate waarin besluitvorming, gedrag en waarden in lijn zijn met de vastgestelde risicobereidheid.

Binnen HR onderscheiden we de volgende risicohoudingen: (1) risicozoekend, (2) risiconeutraal en (3) risicomijdend.

Risk appetite:

De mate waarin Hogeschool Rotterdam bereid is risico's te accepteren bij het nastreven van haar (strategische) doelen.

De risicobereidheid van HR is de vertaalslag van de risicohouding naar (meetbare) grenzen, criteria en beleidskaders. Deze zijn afgestemd op strategie en doelstellingen en vormen de basis voor besluitvorming. De risicobereidheid wordt periodiek herzien op basis van ontwikkelingen in de interne en externe omgeving.

Risicobehandeling:

De strategie die HR hanteert op basis van de analyse van de geïdentificeerde risico's, rekening houdend met haar risicobereidheid: (1) beheersen, (2) overdragen, (3) vermijden, (4) accepteren of (5) nastreven.

- (1) Beheersen door het veranderen van de waarschijnlijkheid of het veranderen van de gevolgen.
- (2) Overdragen door het delen van het risico.
- (3) Vermijden door te besluiten de activiteit waardoor het risico wordt veroorzaakt, niet uit te voeren of voort te zetten.
- (4) Accepteren van het risico op basis van een onderbouwd besluit.
- (5) Nastreven door het nemen of verhogen van het risico teneinde een kans te benutten.

4. Rollen en verantwoordelijkheden

HR hanteert het Three Lines-model (3LM) als standaard raamwerk voor haar processen. Hierbij is de eerste lijn risico-eigenaar, verantwoordelijk voor de uitvoering van processen, doelrealisatie en de beheersing van risico's. De HR-risicomanager heeft vanuit de tweede lijn de kerntaken adviseren en monitoren op het gebied van hogeschoolbrede risico's.

Medewerkers

Medewerkers signaleren aandachts- en risicopunten en handelen conform de kernwaarden verantwoordelijkheid en rechtvaardigheid.

Managers, teamleiders en projectleiders

Managers, teamleiders en projectleiders doorlopen de risicomanagementcyclus binnen hun activiteiten en projecten, bevorderen risicobewustzijn binnen hun teams en rapporteren periodiek over risico's en beheersmaatregelen in de P&C-cyclus.

Directeuren van organisatieonderdelen

De directeuren dragen binnen de eerste lijn verantwoordelijkheid voor risico's binnen hun eigen PDCA. Zij verhouden zich tot de risicobereidheid van de hogeschool en rapporteren periodiek over risico's en beheersmaatregelen in de P&C-cyclus.

College van Bestuur (CvB)

Het CvB draagt eindverantwoordelijkheid voor risicomanagement, stelt het kader risicomanagement vast en borgt implementatie in de (strategische) besluitvorming. Het CvB stelt de risicohouding en risicobereidheid van de organisatie vast.

Raad van Toezicht (RvT)

De RvT ziet vanuit haar toezichthoudende rol toe op de opzet en werking van het interne risicobeheersings- en controlesysteem van HR.

Auditcommissie van de RvT

De auditcommissie adviseert de RvT en heeft als taak de toezichthoudende rol van de Raad van Toezicht ten aanzien van interne beheersing te ondersteunen en te verdiepen, onder andere gericht op de werking van de interne risicobeheersings- en controlesystemen.³

Proceseigenaar

De proceseigenaar draagt zorg voor processen die in balans zijn tussen waardecreatie, efficiëntie en risicobeheersing, in lijn met de strategische doelen van de hogeschool.⁴ De proceseigenaar stelt de risicobereidheid binnen het proces vast, binnen de kaders van de door het CvB vastgestelde risicohouding en hogeschoolbrede risicobereidheid. De proceseigenaar is tevens risico-eigenaar van de procesrisico's binnen diens proces.

Risicomanager

De risicomanager heeft een tweedelijns adviserende en monitorende functie en faciliteert het proces van risicomanagement dat de hogeschool ondersteunt bij het behalen van de (strategische) doelstellingen. De risicomanager is verantwoordelijk voor het bevorderen van het integreren van risicomanagement in de bestaande bedrijfsactiviteiten en bedrijfsprocessen.

De risicomanager is ondergebracht bij GRCA. De risicomanager heeft op functioneel en inhoudelijk vlak een rechtstreekse lijn naar het College van Bestuur en de Raad van Toezicht.⁵

CISO

De Chief Information Security Officer (CISO) is gepositioneerd binnen het tweedelinsteam Governance, Risk & Compliance (GRC) en is belast met het ontwikkelen, bewaken en coördineren van het informatiebeveiligingsbeleid en standaarden, en bewaakt de samenhang met onder andere het kader risicomanagement. Tevens geeft de CISO (on)gevraagd advies en inhoudelijk een opinie op risicoacceptaties ten aanzien van informatiebeveiligingsrisico's.

BCM-adviseur

De BCM-adviseur is gepositioneerd binnen het tweedelinsteam Governance, Risk & Compliance (GRC) en bewaakt de samenhang tussen Business Continuity Management (BCM), risicomanagement en crisismanagement en draagt zorg voor integrale afstemming met andere veiligheidsthema's en terugkoppeling naar het CvB.

Auditfunctie

De auditfunctie is belegd binnen GRCA, beoordeelt vanuit de derde lijn de samenwerking tussen de eerste lijn en de risicomanager en verstrekt aanvullende assurance ten aanzien van het risicomanagementsysteem binnen HR.

³ Hogeschool Rotterdam, Reglement Raad van Toezicht (2025)

⁴ Notitie Profiel proceseigenaar, 2026

⁵ Hogeschool Rotterdam, Charter risk manager, 2021

5. Het risicomanagementproces

Risicomanagement binnen HR is opgebouwd volgens de principes van COSO ERM 2017 en sluit aan bij de richtlijnen van ISO 31000. De essentie van het risicomanagementproces is terug te brengen tot vijf componenten⁶:

1. Bepalen van de missie, visie en kernwaarden.
2. Formuleren van strategie, doelstellingen en risicobereidheid.
3. Periodiek doorlopen van de risicomanagementcyclus.
4. Jaarlijks reflecteren op het proces en de effectiviteit van maatregelen om risicobewustzijn te versterken.
5. Periodiek communiceren, rapporteren en monitoren.

Door deze componenten systematisch toe te passen binnen alle organisatieonderdelen, draagt het risicomanagementproces bij aan het actief sturen op doelrealisatie, het borgen van continuïteit en kwaliteit en het vergroten van de veerkracht van HR.

De risicomanagementcyclus

De risicomanagementcyclus wordt binnen HR doorlopen op strategisch, tactisch en operationeel niveau binnen alle organisatieonderdelen en binnen alle organisatielagen. Hierbij hanteren we een jaarlijkse, systematische cyclus die bestaat uit:

1. Identificeren van risico's: het signaleren van interne en externe risico's.
2. Analyseren, door het bepalen van impact en waarschijnlijkheid.
3. Beoordelen van de invloed op (strategische) doelen en onze maatschappelijke opgaven.
4. Vaststellen van de risicobehandeling, gebaseerd op de risicobereidheid van HR: beheersen, vermijden, overdragen, of accepteren.
5. Zorgvuldig afwegen en transparant vaststellen van passende beheersmaatregelen.

Risicorapportages

Binnen alle organisatieonderdelen worden risico's systematisch vastgelegd, gerapporteerd en opgevolgd als integraal onderdeel van de PDCA-cyclus en de planning- en controlcyclus. Proceseigenaren, directeuren en managers in de eerste lijn zijn verantwoordelijk voor het bijhouden van een actueel risicoregister, waarin per risico ten minste de risicobeschrijving, risico-eigenaar, impact, waarschijnlijkheid, voorgenomen risicobehandeling en eigenaar van de beheersmaatregelen (indien van toepassing) zijn opgenomen. Zij bespreken de belangrijkste risico's en bijbehorende beheersmaatregelen periodiek in hun eigen overlegstructuren en rapporteren hierover ten minste jaarlijks, en bij significante wijzigingen tussentijds, in de reguliere P&C-cyclus (jaarplannen, reviewrapportages, overige managementrapportages). In de rapportages wordt een korte evaluatie opgenomen van de effectiviteit van getroffen maatregelen en eventuele aanvullende acties. De risicomanager bewaakt in de tweede lijn de samenhang en volledigheid van de risicorapportages en adviseert proceseigenaren en directeuren over verbeteringen in de duiding en opvolging van risico's. Het CvB ontvangt op basis van de geaggregeerde risicorapportages een hogeschoolbreed overzicht van de belangrijkste strategische, tactische en (indien van toepassing) operationele

⁶ COSO, Enterprise Risk Management, Integrating with Strategy and Performance, 2017

risico's, inclusief informatie over beheersing en restrisico's, en betreft deze expliciet bij de (strategische) besluitvorming.

6. Risicohouding en risicobereidheid

Risicohouding en risicobereidheid geven richting aan de afweging tussen kansen, risico's en organisatiedoelstellingen, en vormen daarmee een belangrijk instrument voor sturing en besluitvorming. Dit kader risicomanagement biedt het overkoepelende kader voor het bepalen en uitwerken van de risicobereidheid binnen de organisatie. Om dit effectief te verankeren in de hele organisatie, wordt in onderliggende visie-, strategie- en beleidsdocumenten beschreven welke risicobereidheid voor het betreffende beheersgebied geldt en hoe deze zich verhoudt tot de in dit kader vastgelegde uitgangspunten.

Compliance wet- en regelgeving

De **risicohouding** ten aanzien van compliance is risicoavers: het naleven van wet- en regelgeving staat centraal en overtredingen worden actief voorkomen. De **risicobereidheid** is zeer laag: risico's op niet-naleving worden in beginsel niet geaccepteerd. Uitzonderingen zijn slechts mogelijk indien deze wettelijk zijn toegestaan, expliciet zijn afgewogen en passende beheersmaatregelen zijn getroffen.

HR hanteert de volgende risicohouding op de te onderscheiden beheersgebieden:

Onderwijs

De **risicohouding** ten opzichte van onderwijs is **neutraal**: risico's worden expliciet afgewogen tegen kwaliteit, studeerbaarheid en rechtmatigheid. De risicobereidheid is laag tot gematigd: alleen beperkte, onderbouwde risico's die aantoonbaar bijdragen aan onderwijskwaliteit en -innovatie worden geaccepteerd; risico's die continuïteit, accreditatie of naleving die compliance met wet- en regelgeving kunnen schaden, worden in principe niet genomen.

Onderzoek

De **risicohouding** in onderzoek is zoekend: de organisatie stimuleert vernieuwing en experimenteerruimte binnen vooraf gestelde kaders. De **risicobereidheid** is gematigd: de organisatie is bereid risico's te accepteren die inherent zijn aan onderzoek en innovatie, zolang deze beheerst zijn en passen binnen de kaders van onderzoeksintegriteit, ethiek, veiligheid, informatiebeveiliging, kennisveiligheid, privacy en financiële haalbaarheid. Risico's die deze kaders overschrijden worden niet geaccepteerd.

Fysieke omgeving

De **risicohouding** ten aanzien van de fysieke omgeving is mildend: de organisatie stelt veiligheid, gezondheid en de continuïteit van gebouwen en voorzieningen centraal en richt zich primair op het voorkomen van verstoringen en incidenten. De **risicobereidheid** is laag: alleen beperkte risico's worden geaccepteerd wanneer deze noodzakelijk zijn voor de bedrijfsvoering, adequaat zijn beheerst en niet leiden tot onaanvaardbare gevolgen voor veiligheid, gezondheid, continuïteit of financiële stabiliteit. Risico's die kunnen resulteren in onveilige situaties, langdurige uitval van voorzieningen of substantieel financieel nadeel worden in beginsel niet geaccepteerd.

(Digitale) informatievoorziening (en privacy)

De **risicohouding** ten aanzien van informatietechnologie is neutraal: de organisatie benut digitale technologie actief ter ondersteuning van onderwijs, onderzoek en bedrijfsvoering en staat open voor innovatie, terwijl zij tegelijkertijd het belang van veiligheid, privacy en continuïteit onderkent. De **risicobereidheid** is laag voor beschikbaarheid, informatiebeveiliging en privacy, en gematigd voor digitale vernieuwing: de organisatie accepteert beheersbare risico's die samenhangen met de invoering van nieuwe technologieën, mits deze risico's expliciet zijn afgewogen en passende beheersmaatregelen zijn getroffen. Security en privacy by design en default zijn hierbij uitgangspunt.

Financiën en administratie

De **risicohouding** in besturing en financiën is mijdend: de organisatie stuurt op continuïteit, rechtmatigheid en integriteit. De **risicobereidheid** is laag tot gematigd: strategische risico's worden alleen genomen wanneer deze transparant, beheersbaar en financieel verantwoord zijn; risico's die de financiële houdbaarheid, governance of naleving van wet- en regelgeving ondermijnen, worden niet geaccepteerd.

Medewerkers

De **risicohouding** ten aanzien van medewerkers is overwegend mijdend waar het gaat om veiligheid, integriteit, sociale veiligheid, Arbo en naleving van wet- en regelgeving. De **risicobereidheid** is hier laag: risico's die kunnen leiden tot onveilige werksituaties, aantasting van (sociale) veiligheid, ongelijke behandeling van medewerkers, of schending van wet- en regelgeving en cao-afspraken worden niet geaccepteerd.

Voor de ontwikkeling, mobiliteit en inzetbaarheid van medewerkers is de **risicohouding** neutraal: er is ruimte voor vernieuwing in rollen, samenwerkingsvormen en HR-instrumenten, mits deze zorgvuldig zijn onderbouwd, transparant worden besloten en de continuïteit van onderwijs, onderzoek en bedrijfsvoering niet in gevaar brengen. De **risicobereidheid** is laag tot gematigd: de organisatie accepteert beheersbare risico's die bijdragen aan duurzame inzetbaarheid, talentontwikkeling en organisatorische wendbaarheid, waarbij tijdelijke inefficiënties, extra investeringen of onzekerheid over het uiteindelijke resultaat acceptabel kunnen zijn.

Referenties

Bestuurs- en beheersreglement (juli 2025)

Branchecode goed bestuur en toezicht in het hbo (2023)

COSO, Enterprise Risk Management, Integrating with Strategy and Performance (2017)

Handboek kwaliteitszorg Hogeschool Rotterdam (2025)

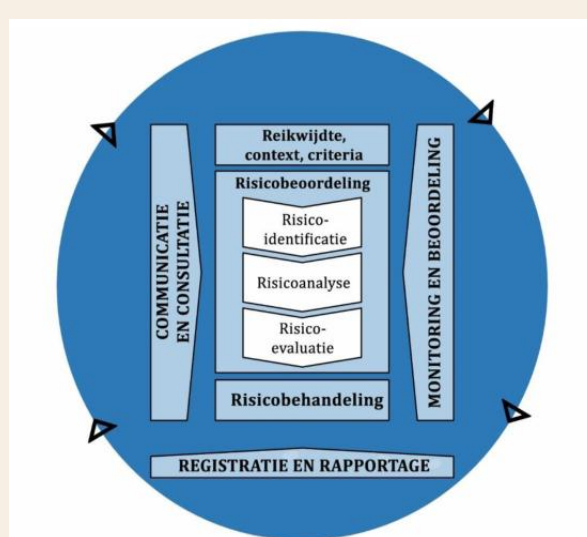
Hogeschool Rotterdam, Charter risk manager (2021)

Hogeschool Rotterdam, Reglement Raad van Toezicht (2025)

Notitie Profiel proceseigenaar (2026)

ISO 31000:2018, Risk management – Guidelines (2019)

Talent voor transitie, Hoger beroepsonderwijs en praktijkgericht onderzoek voor de samenleving van morgen. De Strategische agenda 2023–2028 van de HR



ISO 31000:2018, Risk management – Guidelines (2019)



COSO, Enterprise Risk Management, Integrating with Strategy and Performance (2017)