

Het regelgevende kader voor risicobeheer in het Vlaamse hoger onderwijs is vooralsnog beperkt. Daardoor hebben instellingen de ruimte om hun eigen keuzes te maken. Bart Delmartino beschrijft in grote lijnen hoe (Vlaamse) hogescholen en universiteiten hun risicobeheer kunnen opzetten.

Geef risico-eigenaars het vertrouwen

Een praktische leidraad

Bart Delmartino

KU Leuven

Risicobeheer is een relatief recent beheersproces aan Vlaamse hogeronderwijsinstellingen. Het kwam meer prominent onder de aandacht in antwoord op Vlaamse regelgeving. Dit regelgevend kader blijft zeer beperkt in vergelijking met bijvoorbeeld dat van de financiële of farmaceutische sector.

Het Besluit van de Vlaamse Regering betreffende controle en single audit (2015) stelt in artikel 4: 'Het instellingsbestuur is verantwoordelijk voor de risicoanalyse en het risicomanagement op het niveau van de instelling. (...) De controleactoren evalueren in overleg met het Rekenhof en volgens het principe van de single audit het door de instelling gevoerde risicomanagement.'

Volgens de Codex Hoger Onderwijs (artikel IV.96, zoals gewijzigd in 2019) omvatten de toezichtstaken van de

regeringscommissarissen '1° het door de instelling gevoerde risicomanagement evalueren, in overleg met de externe controleactoren en het Rekenhof. De commissarissen volgen de risicoanalyse van de instelling en de werking van de interne auditororganen op en kunnen opmerkingen formuleren.'

Voordien was risicobeheer aan Vlaamse hogeronderwijsinstellingen beperkt tot een aantal thema's, bijvoorbeeld inzake welzijn op het werk, of werd het niet als dusdanig benoemd. Er was met andere woorden geen holistische en consistente aanpak binnen hogeronderwijsinstellingen, laat staan over instellingen heen.

Brede definities

Er bestaan verschillende definities van risico en risicobeheer. Algemeen kunnen we risico omschrijven als de mogelijkheid dat een gebeurtenis zich voordoet en een impact heeft op de realisatie van de doelstellingen van een instelling; in het geval van een hogeronderwijsinstelling gaat het daarbij om het organiseren van onderwijs, onderzoek en maatschappelijke dienstverlening. Hierbij kan een gebeurtenis zowel een bedreiging als een (gemiste) opportuniteit zijn. Even algemeen is risicobeheer dan het proces om risico's expliciet te identificeren en bewust te beantwoorden, en hierover te rapporteren. Dit proces maakt deel uit van zowel het operationele beheer van een instelling als de strategische cyclus en beleidscyclus. Dergelijke zeer brede definities hebben vooral als doel om het spreken over risico's niet semantisch of anderszins in te perken.

Het regelgevend kader

blijft zeer beperkt

vergeleken met dat van

de financiële sector

Risicomanagement

Een instelling kan risico's slechts duurzaam beheren als ze een goede risicocultuur heeft. Dat betekent enerzijds dat alle medewerkers en organen van de instelling hun verantwoordelijkheden kennen en opnemen op het vlak van risicobeheer en het belang inzien van actief omgaan met risico's en risicoprocessen. Anderzijds moet de instelling het risicobeheer ontwerpen en toepassen op een manier die bij haar past. Als risicobeheer een papieren oefening is, heeft het geen toegevoegde waarde.

Academische cultuur

Een dergelijke risicocultuur is onderdeel van de bredere cultuur van een instelling. In het geval van een hogeronderwijsinstelling is dat in de eerste plaats een academische cultuur. Enkele belangrijke kenmerken daarvan zijn de academische vrijheid, de wil en expertise om onderwerpen in de diepte te doorgronden, de mogelijkheid om theorieën in vraag te stellen en de ruimte om te innoveren. Daarnaast heeft elke instelling een eigen identiteit en cultuur, bijvoorbeeld op het vlak van besluitvorming of leiderschap.

De academische cultuurkenmerken vertalen zich in een aantal uitgangspunten en keuzes voor het risicobeheer binnen een hogeronderwijsinstelling:

- De verantwoordelijkheid voor het omgaan met risico's zit sterk verspreid over de instelling, niet centraal. Elk deel van de instelling (zoals een faculteit of onderzoekseenheid, maar ook een beleids- of beheersdienst) krijgt het vertrouwen om de eigen risico's te beheren. Deze lokale verankering is idealiter gealigneerd met de bestaande organisatie- en managementstructuur, waarbij de taken en verantwoordelijkheden op het vlak van risicobeheer gekoppeld zijn aan de ruimere beleids- en beheersverantwoordelijkheden. Een dergelijke alignering stimuleert de integratie van risicobeheer met andere processen, wat het risicobeheer tastbaarder maakt.
- Het bestuur van de instelling focust op het geconsolideerde risicoprofiel van de instelling en de risico's die raken aan de strategie van de instelling. Op die basis kan het bestuur de globale staat van het risicobeheer aan de instelling beoordelen. Het bestuur heeft een belangrijke voorbeeldrol op het vlak van risicocultuur: de houding in woord en daad van het bestuur als het gaat om risicobeheer – de *tone at the top* – beïnvloedt de houding van de rest van de instelling.
- Een centrale risicofunctie – met risicobeheer als hoofd- of bijzaak, afhankelijk van de omvang van de instelling – focust op ondersteuning, niet op controle. Het gaat enerzijds om ondersteuning van de lokale risico-eigenaars door het aanbieden van een gemeenschappelijk begrippenkader, het begeleiden van workshops, het delen van best practices, het uitwerken van concepten, templates et cetera, afhankelijk

van de risicomaturiteit van de instelling. Hierbij moet de instelling steeds de balans zoeken tussen lokale eigenheid en expertise en centrale consistentie. Anderzijds ondersteunt de risicofunctie het bestuur van de instelling door het aanbieden van een geconsolideerd overzicht van risico's en een analyse van de effectiviteit van de risicobeheersprocessen. Daarnaast biedt de risicofunctie adviesverlening op maat, bijvoorbeeld een diepere analyse van een specifiek (strategisch) risico. De risicofunctie is verwant met de interne-auditfunctie in de zin dat beide gericht zijn op analyse en optimalisatie van activiteiten en processen. Het voornaamste onderscheid is dat de interne audit rechtstreeks verantwoording aflegt aan het bestuur, terwijl de risicofunctie onder het senior management valt en via die weg de risico-eigenaars hiërarchisch meer kan begeleiden in hun beleidskeuzes dan de interne audit. Omwille van effectiviteit en efficiëntie is het belangrijk dat beide functies hun aanpak en planning afstemmen en hun resultaten delen.

- Risicobeheer impliceert geen risico-aversie. Onderzoek en innovatie zijn niet mogelijk zonder risico. Risicobeheer faciliteert onderzoek en innovatie door ervoor te zorgen dat medewerkers risico's kennen en er bewust mee omgaan, waarbij een instelling kan kiezen om een risico te aanvaarden en te laten bestaan. Om het risicobeheer te sturen of om risico-eigenaars net expliciet te responsabiliseren, kan een instelling haar risico-appetijt formuleren: de aard of hoeveelheid risico die de instelling wil aanvaarden. Deze risico-appetijt vormt dan het kader waarbinnen de instelling specifieke risico's kan beheren. Risico-appetijt is een keuze van de instelling op strategisch-beleidsmatig of operationeel niveau, die ze positief of negatief kan formuleren, kwalitatief of kwantitatief.
- Risicobeheer is geen mechanisch proces dat je volledig kunt vatten in modellen. Er is geen absoluut goed of fout, maar wel ruimte voor *expert opinion* en discussie bij het identificeren van risico's en het formuleren van een risicospons. De identiteit, cultuur en strategie van de instelling zijn van invloed op de keuzes die medewerkers maken. De eerdergenoemde ondersteuning door de risicofunctie zorgt wel voor consistentie en vermijdt willekeur.

Twee kanten van risicobeheer

Zoals gezegd kun je risicobeheer algemeen definiëren als het proces om risico's te identificeren en te beantwoorden, en hierover te rapporteren. Als deel van de strategische cyclus of beleidscyclus van een hogeronderwijsinstelling gaat risicobeheer dan over proactief nadenken over risico's. Als deel van het operationele beheer van de instelling gaat het over het kaderen van concrete incidenten.

Risicomanagement

Strategisch-beleidsmatig

Het is belangrijk voor een instelling, op alle niveaus, om bij het bepalen van de strategische richting en de beleidsmatige implementatie daarvan te weten met welke risico's ze rekening moet houden. Daarom is een periodieke risico-opvolging nodig. Dat houdt in dat de instelling risico's beschrijft, meet in termen van impact en waarschijnlijkheid, beantwoordt en rapporteert.

Bij die opvolging moet ze geen exhaustiviteit nastreven. De aandacht kan uitgaan naar de belangrijkste realistische risico's, om gericht te kunnen handelen en de oefening behapbaar en relevant te houden. Het is wel belangrijk om de hele instelling af te dekken. Dat wil zeggen dat ze de oefening voor de hele instelling maakt, hetzij op basis van het organogram, hetzij op basis van een overzicht van activiteitsdomeinen of -processen.

Gelet op de genoemde uitgangspunten en keuzes voor het risicobeheer binnen een hogeronderwijsinstelling krijgen risico-eigenaars een grote vrijheid bij de opvolging, met beperkte centrale richtlijnen gericht op consistentie en rapportering aan het bestuur van de instelling. Daarbij gaat het onder meer om de volgende richtlijnen:

- Denk voldoende ruim: het risico kan strategisch, operationeel, financieel, reputationeel of compliancegerelateerd zijn.
- Wees concreet, maar niet specifiek dan nodig. Richt je bijvoorbeeld op het risico dat de jaarrekening niet voldoet aan de boekhoudregels, eerder dan op het generieke risico van compliance met regelgeving of het risico niet in lijn te zijn met één specifieke regel.
- Meet impact en waarschijnlijkheid op een eenvoudige manier: een schaal van drie punten voor zowel impact als probabiltiteit kan voldoende zijn en leidt al tot een matrix met negen mogelijke totale 'risicoscores'. Elk van die negen velden is dan een indicator van de relatieve dringendheid of prioriteit waarmee een risico een risicoscorens behoeft. Risicometing is gebaseerd op *expert judgement*, wat een mate van subjectiviteit impliceert. Objectiverende handvatten kun je definiëren

(bijvoorbeeld: een arbeidsongeschiktheid van meer dan x dagen of een aansprakelijkheid van y euro kun je beschouwen als een hoge impact), maar gezien de schaal van de activiteiten en de aard van de risico's van een hogeronderwijsinstelling is het niet realistisch om modelmatige objectiviteit na te streven.

- Formuleer een expliciete en proportionele risicoscorens, minstens voor de risico's met de hoogste dringendheid: die scorens kan zijn om het risico te aanvaarden (geen actie vereist), te vermijden (een activiteit stoppen of niet opstarten), over te dragen (veelal in de vorm van verzekering) of te beperken tot een aanvaardbaar niveau via beheersmaatregelen. De risicoscorens kan focussen op een deel van de oorzaken of gevolgen van het risico, of op een deel van de organisatie. Daarnaast kun je beleidsmatig beslissen om de relatieve prioriteit te overrulen en eerst een antwoord te formuleren op een risico met een lagere risicoscorens, bijvoorbeeld omwille van beperkte middelen, *low-hanging fruit*, verwachtingen van stakeholders et cetera.

Om de risico-opvolging te koppelen aan de strategische cyclus en beleidscyclus van de instelling als geheel, rapporteert de risicofunctie over de overkoepelende resultaten van de oefening aan het bestuur. Deze overkoepelende resultaten geven het risicoprofiel van de instelling weer. Op basis van het opvolgingsproces en de resultaten ervan kan het bestuur dan een uitspraak doen over de staat van het risicobeheer aan de instelling.

Inhoudelijk kunnen de risicofunctie en het bestuur bijzondere aandacht schenken aan strategische risico's, dat wil zeggen: risico's die een impact hebben op de strategie van de instelling of risico's die net onvoldoende op de strategische radar van de instelling staan. Risico-opvolging is aldus een instrument in de opvolging van de bestaande strategie en een input voor het formuleren van een nieuwe strategie. Naast de overkoepelende rapportering over strategische risico's is het aangewezen dat elke risico-eigenaar de specifieke resultaten van de eigen opvolging bespreekt met de verantwoordelijke beleidsmakers, als onderdeel van de reguliere managementrapportering.

Operationeel risicobeheer

Als deel van het dagelijkse operationele beheer moet de instelling adequaat omgaan met concrete incidenten. Vanuit het standpunt van risicobeheer is het belangrijk om deze incidenten daarnaast ook te bekijken als *challenge* van een input voor de periodieke risico-opvolging:

- Is het incident een uiting van een breder risico dat al eerder is geïdentificeerd? Is bijvoorbeeld een ongeval in een labo het gevolg van onvoldoende aandacht voor persoonlijke beschermingsmiddelen? Een bijkomend risico kun je zo nodig identificeren (en beheren) om beter voorbereid te zijn op toekomstige incidenten.

Is het incident een uiting van een breder risico dat al eerder is geïdentificeerd?

Risicomanagement

- Is het incident in lijn met de ingeschatte impact en probabiteit van het risico? Indien niet, dan kun je die inschatting aanpassen om realistischere verwachtingen te creëren of een bijgestelde respons te triggeren.
- Zegt het incident iets over de keuze of implementatie van de beleidsmatig geformuleerde risicorespons? Als het incident suggereert dat de risicorespons niet de juiste is, of de implementatie onvoldoende, kun je de respons aanpassen of de implementatie aanscherpen.

Het is daarom belangrijk om incidenten enerzijds consequent en expliciet te registreren en anderzijds bewust te linken aan de periodieke risico-opvolging.

De resultaten van het operationele risicobeheer maken deel uit van de reguliere managementrapportering. Daarnaast kun je eventuele conclusies meenemen in de volgende periodieke opvolging. Zeker wat de risicorespons betreft moet je echter niet wachten om de respons of de implementatie ervan bij te stellen.

Onderstaande tabel geeft een korte samenvatting van strategisch-beleidsmatig en operationeel risicobeheer:

	Strategisch-beleidsmatig	Operationeel
Identificatie	Periodieke zelfreflectie en bevraging met betrekking tot reële en potentiële risico's	Bekijken of je concrete incidenten kunt koppelen aan geïdentificeerde risico's
Meting	Inschatten van impact en probabiteit van risico's	Bekijken of concrete incidenten in lijn liggen met de ingeschatte impact en probabiteit
Respons	Beslissen om een risico te aanvaarden, te vermijden, over te dragen of te beperken	Evalueren of de risicorespons adequaat is (juiste respons en effectieve implementatie)
Rapportering	Bestuur informeren over risicoprofiel, met focus op strategische risico's	Management informeren over concrete incidenten en hun link met de risico-opvolging

Tabel 1 Strategisch-beleidsmatig en operationeel risicobeheer

Ruimte voor eigen keuzes

Hogeronderwijsinstellingen hebben, minstens in Vlaanderen, ruimte om hun eigen keuzes te maken op het vlak van risicobeheer. Ons basisidee is dat duurzaam risicobeheer aan hogeronderwijsinstellingen moet passen in hun academische cultuur. Dat betekent onder meer dat risico-eigenaars het vertrouwen krijgen om binnen een instellingsbreed beleidskader hun eigen risico's lokaal te beheren. Dat beheer omvat zowel proactief nadenken over risico's als het kaderen van concrete incidenten.

Bart Delmartino

is risicomanager en directeur van de Directie Stafdiensten Algemeen Beheer van KU Leuven