

Integraal Risicomanagement in het hoger onderwijs, naar een Integrale Veiligheidsinfrastructuur

Hoe herkenbaar zijn onderstaande 7 stappen uit de ethische lifecycle voor u?



Centrale vragen m.b.t. integraal risicomanagement: Bent u als bestuurder 'in control'?

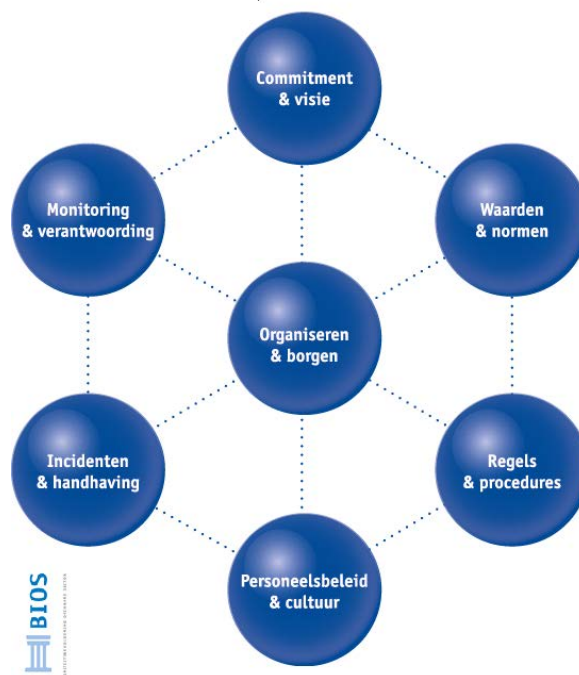
- Heeft u de risico's in kaart?
- Welke risico's bent u tegen gekomen?
- Tegen welke risico's lopen uw medewerkers aan?
- Waardoor werden die veroorzaakt?
- Wat waren de gevolgen?
- En hoe heeft u ze beheersbaar gemaakt?

Geleerde lessen op het terrein van integrale veiligheidsvraagstukken:

- Informatiebeveiliging
- Kennisveiligheid
- Privacybescherming
- Integriteit

Aanpak

Sectorbreed: Integraal en samenhangend.



Bron: BIOS

1. Commitment & visie

Integraal veiligheidsbeleid kan alleen goed slagen als het (top)management van de organisatie het een belangrijk onderwerp vindt, het zichtbaar steunt en bereid is voldoende middelen ervoor vrij te maken. Naast de wil om op integrale veiligheid te sturen en het belang ervan uit te dragen is het noodzakelijk dat de leiding een heldere visie op integrale veiligheid, risicobeheersing en risicomangement formuleert. Vragen die daarbij bijvoorbeeld van belang zijn: waarom willen we aandacht besteden aan integrale veiligheid, wat verstaan we eronder en wat is onze ambitie?



2. Waarden & normen

Waarden en normen vormen het geheel van geschreven en ongeschreven regels en maken inzichtelijk waar de organisatie en de medewerkers voor staan en op aangesproken kunnen worden. Ze vormen de basis onder het integraal veiligheidsbeleid, waaronder het integriteitsbeleid. Hier gaat het om vragen als: 'Kan dit wel?', 'Mag dit wel?' of 'Wil ik dit wel?'. Het is van belang om de waarden en normen van de organisatie vast te leggen in een gedragscode. Relevante thema's die daarin aan de orde kunnen komen zijn bijvoorbeeld: wat zijn onze kernwaarden, wat zijn de algemene spelregels ten aanzien van veel voorkomende veiligheids- en integriteitskwesaties, waaronder fraude, belangenverstrengeling, wetenschappelijke integriteit, kennisveiligheid en informatiebeveiliging, en bij wie kunnen de medewerkers en studenten terecht met concrete vragen. Hoe zorgen bestuurders voor een veilig klimaat voor studenten en medewerkers. Hoe tonen leidinggevenden voorbeeldgedrag en voorkomen bestuurders overregulering zonder daarbij in voorkomende gevallen een gevoel van gepaste alertheid en bij het omgaan met incidenten de 'sense of urgency' uit het oog te verliezen.



3. Regels & procedures

De waarden en normen worden geconcretiseerd en ondersteund door het geheel van formele regels en procedures in de organisatie en vinden hun weerslag in de interne Administratieve Organisatie en Interne Controle. Thema's die daarin van belang zijn, zijn bijvoorbeeld: de opzet van interne toezicht- en auditsystemen, beschrijvingen van werkprocessen en risicobeheersende maatregelen zoals het vier-ogen-principe, functiescheiding en -rotatie, het bestuur- en beheersreglement, vigerende wet- en regelgeving (ABW, WHW en overig¹), branche- en gedragscodes en studentenstatuut.² Een ander punt van aandacht is daarbij regelmatig na te gaan of bestaande regels en procedures werken en doen wat ze moeten doen om te voorkomen dat je voor verrassingen komt te staan als ze moeten werken. Effectiviteit hangt immers samen met integraliteit.



¹ Zie overzicht DP Governance

² Nader te specificeren voor hogescholen en universiteiten

4. Personeelsbeleid & cultuur

Aandacht voor integrale veiligheid, waaronder aandacht voor integriteit, is een belangrijk onderdeel van het personeelsbeleid.

Het begint al bij de werving en selectie van personeel. Is screening noodzakelijk en zo ja hoe ver ga je? Ook in diverse personeelsgesprekken (jaarplan, voortgangs- en beoordelings- en exitgesprek) is integriteit een onderwerp dat niet mag ontbreken. Daarnaast zijn ambtseedsessies, introductiebijeenkomsten, werkoverleggen en integriteitstrainingen aangewezen momenten om te werken aan het verbeteren van de cultuur van de organisatie en het bewustzijn van de medewerkers. Het is een kwestie van cultuur in organisaties.

Bewustzijn van de veiligheidsrisico's in het hoger onderwijs is een zaak voor alle betrokkenen, bestuurders, medewerkers en studenten.



5. Monitoring & verantwoording

Het monitoren van het integraal veiligheidsbeleid is noodzakelijk om de voortgang en werking van het integraal risicomanagementsysteem bewaken. Het management kan op basis van de monitorinformatie volgen of de gestelde doelen worden gehaald of dat zij moet bijsturen. Door evaluatiemomenten in te bouwen krijgt de organisatie niet alleen zicht op de werking van de maatregelen, maar kan zij deze ook verder verbeteren. Evaluaties en rapportages zijn vormen van managementinformatie en -verantwoording over de implementatie en de effectiviteit van het integriteitsbeleid.

De Code Goed bestuur van hogescholen is onlangs vastgesteld³. In de nieuwe code zijn de aanbevelingen verwerkt van de commissie Van Montfort, die in opdracht van het bestuur van de Vereniging Hogescholen de governancecode heeft geëvalueerd. Gebleven zijn de verplichting tot het hebben van een integriteitcode, een klokkenluidersregeling en een regeling ongewenst gedrag als onderdelen van een risicomanagement systeem. Nieuw in de Code goed bestuur is de verplichting voor het CvB om in het jaarverslag inzicht te geven in de werking en de belangrijkste resultaten van dat interne risicomanagementsysteem. Daarmee wordt een belangrijke kwaliteitsslag gemaakt in de transparantie van bestuur en toezicht. De tools en processen zijn aanwezig en worden verder ontwikkeld. Nu gaat het erom te laten zien dat ze werken en hoe bestuurders in het hoger onderwijs uit oogpunt van compliance en control zichzelf de maat nemen bij kwesties als informatieveiligheid, privacywetgeving, kennisveiligheid en integriteit. De Vereniging van Samenwerkende Nederlandse Universiteiten heeft onlangs ook in haar Code Goed Bestuur opgenomen, dat het college van bestuur een klokkenluidersregeling vaststelt en de interne risicobeheersings- en risicocontrolesystemen voorlegt aan de interne toezichthouder, de raad van toezicht (Code Goed Bestuur Universiteiten, VNSU, 2013). Met de ontwikkelde tools en instrumenten kunnen universiteiten hun kwetsbaarheden en risico's met betrekking tot veiligheidsvraagstukken integraal in kaart brengen en beheersbaar maken.



6. Incidenten & handhaving

Waarden, normen en regels zijn alleen zinvol als iedereen zich eraan houdt. Het aanpakken van schendingen geeft het signaal af dat aan naleving en voorbeeldgedrag (integer handelen) waarde wordt gehecht. Het bekrachtigt de bestaande normen en verkleint het risico op toekomstige schendingen. Het opzetten van handhavingsbeleid, met daarin regels rondom het onderzoek, het sanctioneren en communiceren van (vermoedens van) misstanden/detecteren en beheersbaar maken van risico's is een essentieel onderdeel van het integraal



³ De Code goed bestuur staat op de website van de Vereniging Hogescholen: <http://www.vereniginghogescholen.nl/bedrijfsvoering/goed-bestuur>

veiligheidsbeleid. Voorzieningen gericht op het omgaan met incidenten zoals meldingenregelingen, vertrouwenspersonen en onderzoeksprotocollen maken onderdeel uit van het integraal risicomanagement binnen hogescholen en universiteiten met betrekking tot veiligheidsvraagstukken.

7. Organiseren & borgen

De aandacht voor veiligheidsvraagstukken in het hoger onderwijs, waaronder integriteit en informatie- en kennisveiligheid, dient duurzaam en samenhangend binnen de organisatie georganiseerd en geborgd te worden. Bestuurders zijn integraal verantwoordelijk voor het resultaat van hun instelling. Dit betekent niet alleen dat ze onderwijs en onderzoek van kwaliteit moeten leveren, maar ook dat financiële en ondersteunende systemen op orde moeten zijn. Het hoger onderwijs maakt deel uit van het publieke domein en heeft een maatschappelijke opdracht.⁴ Daarbij horen openheid, transparantie en als bestuurder 'in control' zijn op alle terreinen. Oog hebben voor integrale veiligheid en integer bestuurlijk handelen is essentieel.

Van belang is dat meldingen van integriteitsschendingen bij een onafhankelijk functionaris belegd kunnen worden. Daarbij moet niet alleen gedacht worden aan schendingen van wetenschappelijk integriteit en/of ongewenst gedrag, waarvoor de meeste HO-instellingen vertrouwenspersonen hebben aangewezen. Een beperkt aantal HO-instellingen heeft naast een VP wetenschappelijke integriteit en een VP ongewenst gedrag een vertrouwenspersoon of ombudsman aangesteld die aanspreekbaar is op personele aangelegenheden (dreigende arbeidsconflicten, promovendiproblematiek, fraude, gewetensproblemen, beoordelingen, enz.). Deze vertrouwenspersoon/ombudsman fungeert tevens als het meldpunt in het kader van de klokkenluidersregeling. De vertrouwenspersoon/ombudsman werkt onder ambtsgeheim, is onafhankelijk en valt rechtstreeks onder het College van Bestuur. Personeelsleden kunnen hun zorgen delen met deze functionaris zonder vrees dat de bespreking van het probleem uitlekt. Belangrijk is hierbij dat duidelijk is wie het beleid coördineert, welke actoren hier verder bij betrokken zijn en wat de rol van het management is. Taken, verantwoordelijkheden en bevoegdheden dienen vastgelegd te worden in een integraal veiligheidsbeleidsplan. Een integraal veiligheids-/integriteitsfunctionaris is de aangewezen persoon om dit plan te ontwikkelen, te coördineren en het lijnmanagement te adviseren over de implementatie van het beleid.



Bronnen:

BIOS, Model Integriteitsinfrastructuur, 2013;
VH, Code Goed bestuur hogescholen, 2013;
VSNU, Code goed bestuur universiteiten, 2013;
Advies Commissie Behoorlijk Bestuur, 2013;

⁴ Zie ook: Een lastig gesprek – Advies Commissie Behoorlijk Bestuur, 2013;
<http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2013/09/11/een-lastig-gesprek-advies-commissie-behoorlijk-bestuur.html>