



PLATFORM
INTEGRALE VEILIGHEID
HOGER ONDERWIJS

Een initiatief van de Vereniging Hogescholen en VSNU

TOOLKIT

implementatie IV-framework

Integrale veiligheid

Voorwoord

Beste veiligheidsprofessional,

Voor u ligt de 'Toolkit implementatie IV-framework', een handleiding voor de implementatie van integrale veiligheid in de governance en bedrijfsvoering van uw hoger onderwijsinstelling.

Integrale veiligheid is een proces wat door de hele onderwijsinstelling wordt gedragen, waarbij veiligheidsrisico's inzichtelijk worden gemaakt en met het oog op de continuïteit van de instelling beheersbaar worden gemaakt door een pakket aan samenhangende maatregelen. Deze maatregelen krijgen vorm op basis van een organisatiebrede risicoacceptatie die gebaseerd is op financiën, gedeelde waarden en realiseerbaarheid. Onderdeel van deze aanpak is het besef dat niet alle veiligheidsincidenten voorkomen kunnen worden en dat 100% veiligheid daarmee niet bestaat.

In het hoger onderwijs wordt door instellingen volop samengewerkt in het platform Integrale Veiligheid Hoger Onderwijs om kennis te ontwikkelen en te bundelen in een portfolio en best practises uit te wisselen voor continue professionalisering op het gebied van integrale veiligheid.

Om te voorzien in de behoefte bij instellingen aan concrete adviezen en routes op het gebied van de implementatie van een IV-framework is deze 'Toolkit implementatie IV-framework' opgesteld, gebaseerd op de eerdere toolkit uit 2012. In dit document wordt een blauwdruk geschetst van de verschillende niveaus van integrale veiligheid in de governancestructuur en bedrijfsvoering van de onderwijsinstelling. Tevens wordt daarbij een stappenplan weergegeven om met concrete acties naar een hoger niveau te komen. Zie hiervoor de leeswijzer.

Doorpraten, tips krijgen of advies geven over integrale veiligheid? We nodigen u van harte uit om contact met ons op te nemen. Ga daarvoor naar www.integraalveilig-ho.nl en kom in contact met andere veiligheidsprofessionals uit het hoger onderwijsdomein.

Stafbureau Platform IV-HO

Voorjaar 2021

Inhoudsopgave

3 Leeswijzer

6 Managementssamenvatting

9 DEEL I: HUIDIGE SITUATIE VAN VEILIGHEID IN HET HOGER ONDERWIJS

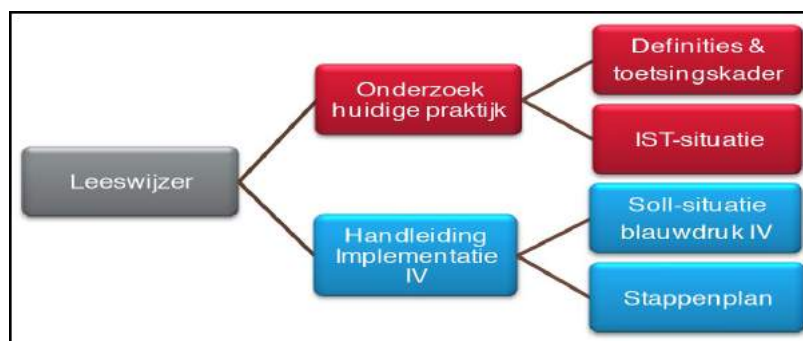
9	1	GOVERNANCE TOETSINGSKADER VOOR INTEGRALE VEILIGHEID
9	1.1	Context
9	1.2	Definitie Integrale Veiligheid
10	1.3	Governance toetsingskader
12	2	DE GOVERNANCE EN BEDRIJFSVOERING VAN INTEGRALE VEILIGHEID
12	2.1	Inleiding
12	2.2	Governance in het algemeen (IST-situatie)
14	2.3	Integrale veiligheid in governance en bedrijfsvoering
14	2.3.1	Strategisch niveau
16	2.3.2	Tactisch / operationeel niveau
21	2.3.3	Verantwoording
22	2.3.4	Toezicht
23	2.4	Mogelijke verklaringen voor huidige governance en bedrijfsvoering van integrale veiligheid

25 DEEL II: IMPLEMENTATIEHANDLEIDING MET STAPPENPLAN

25	3.	BLAUWDRIK VOOR INTEGRALE VEILIGHEID IN DE GOVERNANCE EN BEDRIJFSVOERING
25	3.1	Inleiding
26	3.2	Governance van Integrale Veiligheid (Soll- model)
27	3.3	Rollen in de Soll- Situatie
34	3.4	Bedrijfsvoering van integrale veiligheid
38	4.	STAPPENPLAN NAAR INTEGRALE VEILIGHEID
38	4.1	Inleiding
38	4.2	De ontwikkeling naar integrale veiligheid
40	4.3	Zes categorieën voor de ontwikkeling naar integrale veiligheid
47	BIJLAGE A	AFKORTINGENLIJST
48	BIJLAGE B	STAPPENPLAN INTEGRAAL VEILIGHEIDSRISICOMANAGEMENT

Leeswijzer

De bedoeling van deze leeswijzer is om u als lezer zo snel mogelijk te verwijzen naar de informatie waar u naar op zoek bent. Elk hoofdstuk begint steeds met een overzichtsschema zoals hieronder is weergegeven. Elk hoofdstuk van dit document vormt een bouwsteen, het gekleurde blok geeft aan waar u bent. Dit document bevat twee onderdelen, een onderzoeksgedeelte en een implementatiehandleiding. Het onderzoeksgedeelte is gebaseerd op de uitkomsten van een nulmeting van integrale veiligheid in het hoger onderwijs uit 2012. Als u geïnteresseerd bent in de nulmeting zelf, dan kunt u die op de website van IV-HO terugvinden. Verder wordt in dit document gewerkt met de termen 'ist' en 'soll', die staan voor de huidige situatie (ist) en de toekomstige situatie (Soll).



Deze handleiding is opgebouwd uit vier bouwstenen verdeeld over twee onderdelen:



Onderdeel I. Onderzoek huidige praktijk

- Bouwsteen 1, definities en toetsingskader: Dit onderdeel is een theoretische beschrijving van het toetsingskader voor integrale veiligheid in de governance en bedrijfsvoering binnen universiteiten en hogescholen. Dit onderdeel is relevant indien u meer wilt weten over de definitie van integrale veiligheid, de opbouw van het governance toetsingskader en de verschillende sturingsniveaus.
- Bouwsteen 2, de IST-situatie: Dit onderdeel beschrijft de resultaten van onderzoek naar de huidige inrichting van governance en bedrijfsvoering binnen universiteiten en hogescholen (IST). Leest u vooral dit onderdeel als u meer wilt weten over de verschillende manieren waarop universiteiten en hogescholen op dit moment de veiligheidsfunctie en bedrijfsprocessen daarbinnen hebben vormgegeven. De praktijkvoorbeelden helpen u als lezer inzicht te verkrijgen in de inrichting van de veiligheidsfunctie binnen uw eigen organisatie.

Onderdeel II. Implementatie van Integrale veiligheid

- Bouwsteen 3, de Soll-Situatie: Dit onderdeel schetst een blauwdruk voor het inrichten van integrale veiligheid in de governance en bedrijfsvoering van universiteiten en hogescholen. Deze bouwsteen voorziet in een tweetal benaderingen, die de toekomstige (Soll) situatie beschrijft.
- Bouwsteen 4, het stappenplan: Dit onderdeel tekent de route uit naar inbedding van integrale veiligheid in governance en bedrijfsvoering (van IST naar Soll). Deze bouwsteen geeft u de handvatten om met alle kennis van de voorgaande bouwstenen te combineren en de stappen te doorlopen van de huidige situatie (IST) naar een toekomstige situatie (Soll). Een situatie waarin integrale veiligheid binnen uw organisatie geïmplementeerd is en u als manager of bestuurder de zaken beheerst, 'in control' bent.

Managementsamenvatting

Onderdeel 1. Onderzoek naar de huidige praktijk

Veiligheid in de governance van de hoger onderwijsinstellingen en governance van veiligheid in het hoger onderwijs kent vele vormen en gedaanten. Voor het opstellen van deze handleiding zijn twaalf hogescholen en universiteiten onderzocht. Hieruit kwam naar voren dat ok al kennen zij elk een eigen dynamiek en identiteit, zij op hoofdlijnen een heel duidelijk vergelijkbare governancestructuur hebben. Er zijn grofweg twee sturende organen: het College van Bestuur en de directeuren/decanen. Daarnaast zijn er nog twee adviserende organen: het College van directeuren/decanen en de ondersteunende (facilitaire) dienst.

Uit het onderzoek bleek het volgende:

- mbt strategisch niveau: Elke kennisinstelling kent voor haar organisatie een missie en een visie. Deze algemene missie en visie komen erop neer dat de kennisinstelling ernaar streeft een volwaardige leer-, onderzoeks- en werkomgeving te zijn. Veelal ontbreekt een missie en visie over veiligheid op strategisch niveau. Dit betekent dat er geen sprake is van doorvertaling naar meetbare strategische doelstellingen. Er is wel één algemene overeenkomst te herleiden: de instellingen hebben veelal een veiligheidsbeleid dat gericht is op safety en deze is meestal wetgeving-gestuurd. We constateren een groeiende aandacht voor moedwillig veroorzaakte veiligheidsincidenten in en rondom de instelling (security). Daar waar er sprake is van een veiligheidsfunctionaris binnen een instelling, zien we bij de onderzochte instellingen bijna altijd een ontkoppeling van deze functie ten opzichte van de rest van de veiligheidsorganisatie.
- mbt tactisch/operationeel niveau: Voor het tactisch/operationeel niveau is gekeken naar vijf rollen:
 - o de coördinerende rol,
 - o de uitvoerende rol,
 - o de besluitvormende rol,
 - o de adviserende rol en
 - o de monitorende rol.

Deze rollen geven inzicht in het karakter van de functionarissen die een verantwoordelijkheid hebben voor veiligheid. Binnen de instellingen zijn naast rollen en functionarissen ook overleggremia aanwezig ten aanzien van het onderwerp veiligheid. Het doel van deze overleggremia is om afstemming te realiseren ten aanzien van de implementatie van veiligheidsmaatregelen en de voortgang te bewaken. Het onderzoek laat vier inrichtingsvarianten zien, te weten mono-facultair, staf-facultair, multi-facultair en interfacultair. De onderzochte instellingen tonen een grote variëteit aan instrumenten en maatregelen om handen en voeten te geven aan het thema veiligheid.

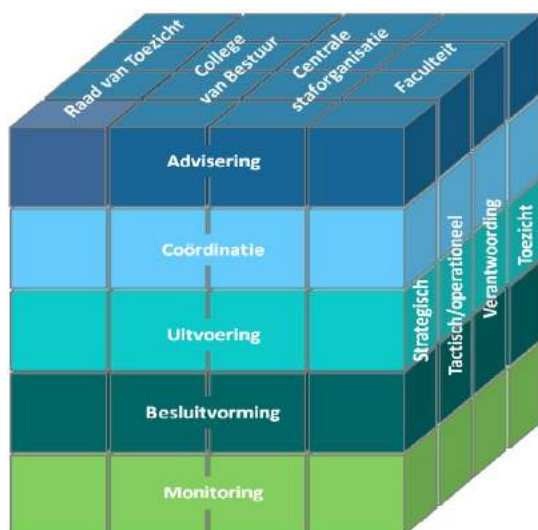
- mbt verantwoording: Door de afwezigheid van een visie (integrale) veiligheid vindt er ook onvoldoende verantwoording plaats op strategisch niveau (College van Bestuur en Raad van Toezicht). De afwezigheid van strategische verantwoording wordt ook versterkt door het feit dat veiligheid onvoldoende onderdeel is van een algeheel PDCA-cyclus.
- mbt toezicht: In dit onderzoek is een onderscheid gemaakt tussen intern en extern toezicht. Intern toezicht vindt veelal op drie niveaus plaats: RI&E, interne audits en toezicht door Raad van Toezicht. Extern toezicht vindt plaats door middel van vergunningverlening en we constateren bij sommige instellingen dat er sprake is van wat wij 'vrijwillig' toezicht noemen: het zelf organiseren van extern toezicht door externe bureaus.

Veiligheid is van oudsher een secundair proces binnen een kennisinstelling. De kwaliteit van de organisatie wordt van nature afgemeten aan onderzoek en onderwijs, veiligheid is daarbij geen criterium. Dit wordt nog eens versterkt door drie verschillende vormen van autonomie bij de decanen/directeuren: juridische (instellingsbesluiten), financiële (budgetverantwoordelijkheid) en informele (gezag) autonomie.

Onderdeel 2. Handleiding voor implementatie van integrale veiligheid

In de implementatiehandleiding wordt, met behulp van onderstaand governance-toetsingskader, invulling gegeven aan de elementen van een driedimensionaal model met op de x-as de verschillende rollen in de organisatie, op de y-as de functiegroepen in de organisatie en op de z-as de categorieën uit de governance structuur.

Figuur 1. Driedimensionale governance model



Op basis van het onderzoek zijn twee blauwdrukken ontwikkeld voor integrale veiligheid het hoger onderwijs.

De eerste blauwdruk richt zich op de governance van integrale veiligheid. Dit is een blauwdruk voor een aansturingsmodel op strategisch en tactisch/operationeel niveau. Deze blauwdruk geeft weer hoe de vijf rollen (coördinatie, uitvoering, besluitvorming, advisering en monitoring) op het thema integrale veiligheid binnen het algemene governance model kunnen worden belegd, zodanig dat ze elkaar versterken en er een bestuurlijk optimum gecreëerd wordt.

De tweede blauwdruk beschrijft de bedrijfsprocessen die in de bedrijfsvoering van de organisatie moeten worden doorgevoerd om integrale veiligheid te kunnen sturen en beheersen. Dit zijn generieke processen voor de traditionele functionele veiligheidsgebieden zoals: arbo, safety, security, milieu, ICT. Ieder van deze functionele veiligheidsgebieden krijgt te maken met processen zoals beleidsvorming, organisatie en handhaving, risico-inventarisatie en sturing, crisismanagement, continuïteitsmanagement en bewustwording. Deze blauwdruk gaat uit van coördinatie en afstemming ten aanzien van deze processen.

Stappenplan naar integrale veiligheid

Om integrale veiligheid goed te implementeren moet de organisatie zowel naar de governance (beleid) als naar de bedrijfsvoering (uitvoering) kijken. In de eerste plaats is de wijze waarop een onderwijsinstelling deze twee pijlers heeft georganiseerd bepalend. Daarnaast bepaalt de ambitie in grote mate welke stappen moeten worden doorlopen. In deze handleiding wordt een dynamisch stappenmodel beschreven dat een onderwijsinstelling helpt bij het bepalen van de benodigde activiteiten voor het realiseren van integrale veiligheid. Het model is flexibel en kan ondersteuning bieden aan alle instellingen, ongeacht het volwassenheidsniveau op het gebied van veiligheid.

Op basis van vijf groeifasen wordt beschreven wat de vereisten aan governance en bedrijfsvoering zijn voor het realiseren van integrale veiligheid. Er wordt onderscheid gemaakt in functionele veiligheid, procesmatige veiligheid, systematische veiligheid, beheerste veiligheid en integrale veiligheid. Dit stappenplan is daarmee een hulpmiddel voor beoordeling van de huidige situatie. Op basis van een zelfanalyse kunnen veiligheidsmanagers bepalen welke onderdelen zij wel en welke zij niet willen oppakken.

Het stappenplan geeft richting aan de te ontwikkelen activiteiten en biedt een houvast voor monitoring van de verbetering op het gebied van integrale veiligheid. Op basis van het toetsingskader en de cruciale processen van integrale veiligheid zijn van zes categorieën van groei af te leiden:

1. Veiligheidsbeleid (strategisch),
2. Organisatie en handhaving (tactische en operationeel),
3. Asset inventarisatie en risicomanagement,
4. Prestatiemeting en evaluatie (verantwoording en toezicht),
5. Crisismanagement en continuïteitsmanagement (tactisch en operationeel) en
6. Bewustwording.

Voor ieder van deze zes categorieën is per ontwikkelfase een set van vragen opgesteld die inzicht geven in de onderdelen van integrale veiligheid.

Deel I: Huidige situatie van Veiligheid in het Hoger Onderwijs

1. Governance toetsingskader voor integrale veiligheid



1.1 Context

De politieke en maatschappelijke discussie omtrent de governance in relatie tot veiligheid in het onderwijs, vindt haar oorsprong in de toename en het soort van het aantal incidenten (en daarmee de gepaard gaande toename van de politieke en media-aandacht). De positie van het onderwijs in het maatschappelijk veld, de toename van de mondigheid van de burger en de toenemende media-aandacht, zijn voorbeelden van ontwikkelingen die zorgen dat de organisationele condities van een onderwijsinstelling moeten voldoen aan geaccepteerde richtlijnen en wensen. Een andere ontwikkeling is die van de terugtrekkende overheid en dat instellingen zich niet meer kunnen beroepen op controle door de overheid en derhalve zelf meer verantwoordelijkheid moeten gaan nemen. Deze toenemende aandacht voor governance in het onderwijsdomein, brengt met zich mee dat ook de aandacht voor governance van integrale veiligheid in het onderwijsdomein toeneemt.

1.2 Definitie Integrale Veiligheid

Veiligheid binnen onderwijsinstellingen is de laatste tijd steeds meer een governance en bedrijfsvoerings-vraagstuk van geworden.

Van oudsher zijn functionele scheidingen in de organisatie van veiligheid waar te nemen (arbo, safety, security, informatie). We kunnen dit duiden als functionele veiligheid. De laatste jaren zien we daarbij een toenemende aandacht voor een aparte veiligheidsfunctionaris binnen onderwijsinstellingen ontstaan. Kenmerk van functionele veiligheid is de aanwezigheid van een hoog professionaliteitsniveau binnen de functionele kolommen en het benoemen van risico's per functionele kolom. Nadeel van deze aanpak is dat dit voor de bestuurder een gefragmenteerd en soms onbeheersbaar beeld van veiligheid oplevert.

"Integrale veiligheid daarentegen is een aanpak om grip te krijgen op alle incidenten en veiligheidsrisico's (exclusief dynamische risico's, zoals economische, politieke en juridische risico's voor een organisatie) in samenhang met elkaar en om gepaste maatregelen in samenhang en d.m.v. samenwerking te nemen. Integrale veiligheid maakt gebruik van gemeenschappelijke processen, zodat een gemeenschappelijk overkoepelend beeld van de veiligheidssituatie ontstaat, ongeacht of er sprake is van arbo, safety, security of IT-risico's . Integrale veiligheid maakt beheersing en besturing van alle veiligheidsfuncties beter en levert concurrentievoordeel op."



Figuur 2. Bouwstenen integrale veiligheid

1.3 Governance toetsingskader

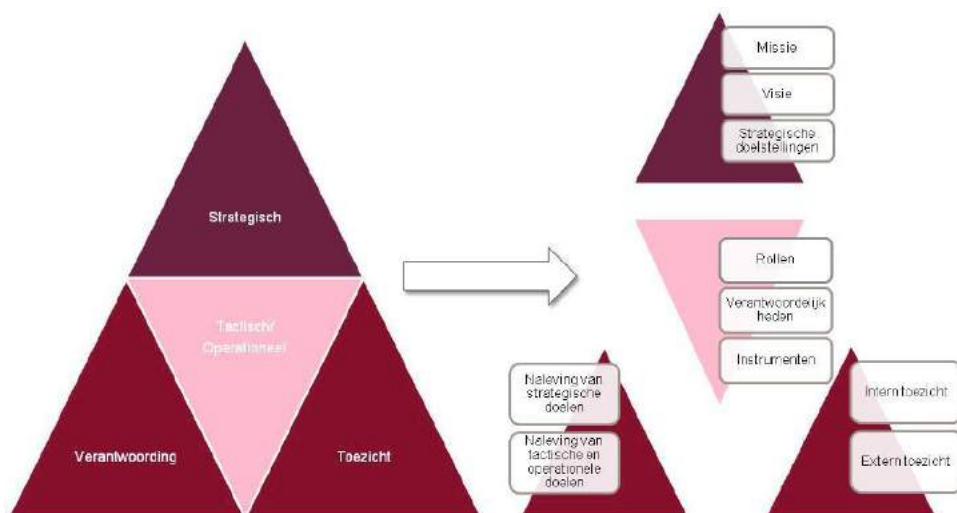
Prof. Dr J. Strikwerda heeft in zijn artikel over educational governance een visie beschreven hoe de algemene notities van good governance vertaald moeten worden in educational governance².

'Om zulke goede condities in actuele, maar ook op langere tijd te creëren, in stand te houden en tijdig aan te passen aan veranderende omstandigheden is bestuur nodig van onderwijsinstellingen. Omgekeerd heeft het bestuur (in de breedste zin van het woord, ouders, maatschappelijke organisaties, overheden) weer een goede organisatie nodig om de kwaliteit van het onderwijs te kunnen beoordelen, te kunnen bijsturen waar dat nodig is en nieuw beleid te kunnen implementeren. Daarnaast heeft het bestuur (in juridische zin, van een rechtspersoon) een goede organisatie nodig om de waarden van de rechtspersoon waarin het onderwijs is georganiseerd zorgvuldig te kunnen beheren en te beschermen en om daarover verantwoording te kunnen afleggen.'

De toenemende aandacht voor governance in het onderwijsdomein, brengt met zich mee dat ook de aandacht voor governance van veiligheid in het onderwijsdomein toeneemt. Immers, de organisationele condities dienen ook een positief effect te hebben op het borgen van integrale veiligheid binnen een kennisinstelling. Vandaar ook dat dit onderzoek een eerste stap is om integrale veiligheid een geïntegreerd onderdeel te laten worden van de governance.

De wijze waarop veiligheid in de governance en bedrijfsvoering van een instelling terugkomt verschilt per onderwijsinstelling. Of hiermee sprake is van integrale veiligheid is op voorhand niet te zeggen. Om de wijze waarop veiligheid is verankerd, in de verschillende governance structuren van universiteiten en Hogescholen te onderzoeken is een toetsingskader opgezet.

¹ Strikwerda, J. 2005. "Goed bestuur van onderwijs: Principes voor educational governance". In F. H. J. G. Brekelmans, P. W. A. Huisman, & J. M. M. v. d. Ven (Eds.), Educational Governance - Symposiumbundel Nederlandse Vereniging voor Onderwijsrecht 2004, Vol. 24: 17-34. Den Haag: Sdu.



Figuur 3. Toetsingskader

In bovenstaand model worden vier categorieën weergegeven die samen de governance structuur en interne beheersing/bedrijfsvoering van de onderwijsinstelling beschrijven:

- **Strategisch.** Het betreft hier de functie van leiderschap om richting te geven aan de organisatie en waarbij uitdagingen worden aangegaan en verliezen worden vermeden. Het strategische deel van het toetsingskader wordt geïnventariseerd op basis van drie elementen: missie, visie en strategische doelstellingen.
- **Tactisch/operationeel.** Het betreft hier de tactisch/operationele keuzes die gemaakt zijn om integrale veiligheid te borgen en daar waar nodig onveiligheid tijdig te signaleren en de adequate reactie erop. Het tactische niveau borgt de samenhang en integraliteit van de verschillende elementen. Het operationele deel van het toetsingskader wordt geïnventariseerd op basis van drie deelelementen: rollen, verantwoordelijkheden en instrumenten.
- **Verantwoording.** Het betreft hier de verantwoording van de 'tactisch/operationele' organisatie van de uitvoering van taken en de naleving ervan. Dit deel van het toetsingskader wordt geïnventariseerd op basis van twee deelelementen: naleving strategische doelen en naleving tactisch/operationele doelen.
- **Toezicht.** Het betreft hier het toezicht op het strategisch niveau (leiderschap) en de 'tactisch/operationele' organisatie van de naleving ervan. Dit deel van het toetsingskader wordt geïnventariseerd op basis van twee deelelementen: intern toezicht en extern toezicht.

In dit hoofdstuk heeft u kunnen lezen waarom integrale veiligheid verschilt van functionele (gefragmenteerde) veiligheid. Door gebruik te maken van gemeenschappelijke processen ontstaat een gemeenschappelijk overkoepelend beeld van de veiligheidssituatie. Dit maakt het mogelijk om alle veiligheidsfuncties in samenhang te beheersing en te besturen. De manier waarop sturing en beheersing binnen een organisatie zijn ingericht (governance), verschilt per instelling. Het toetsingskader is een versimpeling van de werkelijkheid. Het vormt de bril waarmee in deze handleiding naar de governance structuur van onderwijsinstellingen wordt gekeken. Het helpt in te zoomen op specifieke probleemgebieden en het geeft structuur aan de bevindingen die in de hiernavolgende bouwstenen worden besproken. Met het bestuderen van deze eerste bouwsteen heeft u kennis kunnen maken met de definitie van integrale veiligheid en het toetsings- kader voor governance en sturing binnen instellingen voor hoger onderwijs.

2. De governance en bedrijfsvoering van integrale veiligheid



2.1 Inleiding

Governance van veiligheid in het hoger onderwijs kent vele vormen en gedaanten. In dit hoofdstuk worden de vier categorieën governance (strategie, tactisch/operationeel, toezicht en rapportage) uitgewerkt. Dit hoofdstuk is als volgt opgebouwd.

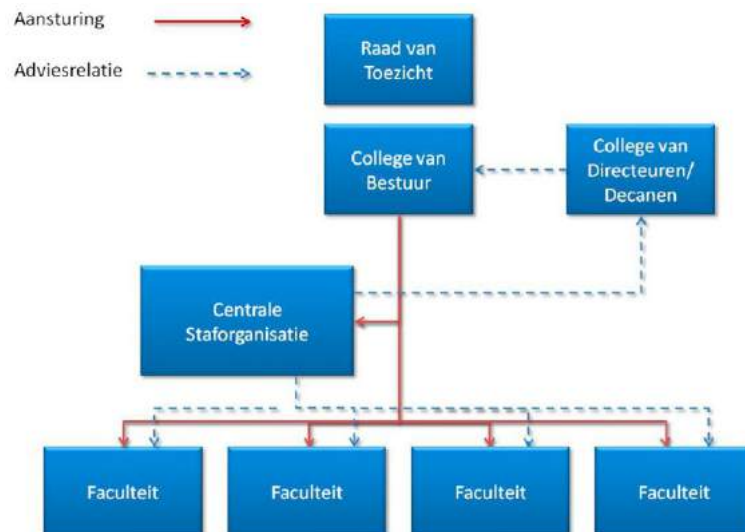
Dit hoofdstuk bestaat uit drie delen. Ten eerste de algemene governance en bedrijfsvoering zoals dat is aangetroffen bij de instellingen (paragraaf 2.2). Ten tweede de integrale veiligheid in de governance en bedrijfsvoering van de instellingen (paragraaf 2.3). Ten derde mogelijke verklaringen voor de inrichting van de governance en bedrijfsvoering van integrale veiligheid (paragraaf 2.4).

2.2 Governance in het algemeen (IST-situatie)

De hogescholen en universiteiten die bij het onderzoek ten behoeve van deze handleiding zijn betrokken hebben op uitvoeringsniveau elk een eigen dynamiek en identiteit. Wij herkennen op hoofdlijnen een heel duidelijk vergelijkbare governancestructuur.

Er zijn grofweg twee sturende organen: Het College van Bestuur en de decanen/directeuren³. Daarnaast zijn er nog twee adviserende organen: het college van directeuren en decanen en de ondersteunende/facilitaire dienst. In het schema hieronder is die hoofdstructuur globaal weergegeven.

² Voor universiteiten en hogescholen worden verschillende benamingen gehanteerd voor de beheerseenheid die verantwoordelijk is voor een specifiek onderdeel van onderzoek en onderwijs. De benamingen zijn faculteiten, directies, academies en onderzoeksscholen. De beheerders van deze entiteiten vertonen ook verschillen. Voor de leesbaarheid spreken we in deze handleiding van faculteiten (voor zowel universiteiten als hogescholen) als het om de entiteit gaat en om decanen/directeuren als het om de verantwoordelijke beheerders gaat.



Figuur 4. Hoofdstructuur governance

De Raad van Toezicht

De Raad van Toezicht is belast met het toezicht op de continuïteit en belangen de gehele organisatie. Gezamenlijk met het College van Bestuur is de Raad van toezicht verantwoordelijk voor de corporate governance structuur van de organisatie. De Raad richt zich, conform de wet³, bij de vervulling van haar taak naar de belangen van de organisatie, in evenwicht met belangen van de bij de kennisinstelling betrokken instanties, organisaties en personen en overeenkomstig de visie op de maatschappelijke positie van de organisatie.

Aan de Raad van Toezicht zijn taken opgedragen als:

- de goedkeuring van het instellingsplan
- de begroting en het bestuurs- en beheersreglement
- het jaarverslag

Het College van Bestuur

Het College van Bestuur (CvB) is het hoogste bestuursorgaan van de organisatie. Het College van Bestuur is verantwoording verschuldigd aan de Raad. Zij bepaalt de visie van de instelling en stuurt middels meerjarenplannen en visiedocumenten de onderwijsinstelling als geheel en de verschillende onderdelen van de onderwijs- instelling in het bijzonder aan.

Het College van Bestuur heeft directe lijnen met de diverse faculteiten en wordt ondersteunend door de ondersteunende/facilitaire diensten. Het College van Bestuur stuurt de verschillende onderdelen aan en heeft contact met de Decanen (universiteiten) of Directeuren(hogescholen). Het College van Bestuur wordt gecontroleerd door de Raad op haar bestuurlijke werkzaamheden en de financiën van de onderwijsinstelling.

Decanen/directeuren

Decanen/directeuren zijn verantwoordelijk voor het bestuur en het beheer van de faculteit, het onderwijscluster of Dienst. De decanen/directeuren hebben voor het uitvoeren van hun taak het mandaat van het College van Bestuur. De daaruit voortvloeiende taken en functies voert de decaan/directeur uit in collegiaal overleg met het faculteitsbestuur waarvan hij voorzitter is. Het faculteitsbestuur behartigt de dagelijkse gang van zaken van de faculteit.

³ Het betreft hier de Wet op het Hoger Onderwijs en Wetenschappelijk Onderzoek ("WHW")¹

Het College van Decanen heeft een adviserende functie richting het College van Bestuur.

Ondersteunende/ facilitaire dienst

De ondersteunende/facilitaire dienst ondersteunt de faculteiten/ clusters bij de uitvoering van hun primaire taken op het gebied van onderwijs en onderzoek. De ondersteunende/facilitaire dienst ondersteunt de faculteiten in de PIOFAH-bedrijfsprocessen⁵ en adviseert op het gebied van milieu en veiligheid en houdt zich bezig met het beheer van de vastgoedportefeuille van de universiteit.

2.3 Integrale veiligheid in governance en bedrijfsvoering

2.3.1 Strategisch niveau

Elke instelling kent voor haar organisatie een missie en een visie. Kort samengevat komt deze algemene missie en visie erop neer dat de instelling ernaar streeft een volwaardige leer-, onderzoeks- en werkomgeving te zijn. Zowel voor studenten als voor medewerkers. Dit wordt vaak vertaald in strategische doelstellingen. Een voorbeeld van een visie is als volgt:

De universiteit is ambitieus in wetenschappelijk onderzoek en onderwijs en stimuleert de vrije en open communicatie van ideeën. De universiteit staat voor universele universitaire waarden als academische vrijheid en onafhankelijkheid.

De visie en missie van instellingen hebben als overeenkomst dat zij de toegankelijkheid en kwaliteit van onderzoek en onderwijs als kernwaarden beschouwen. De inrichting van het strategisch niveau (missie, visie, strategische doelstellingen) ten aanzien van (integrale) veiligheid daarentegen vertoont verschillen tussen de onderzochte kennisinstellingen. Verschillen in de zin dat het geen gemeengoed is om de visie van veiligheid op te nemen in de algemene visie van de kennisinstelling. Althans, niet op strategisch niveau. Als we inzoomen op het operationele niveau, dan zien we bij enkele kennisinstellingen dat bij veiligheidsplannen er uitspraken worden gedaan over het borgen van een veilige leer- en werkomgeving.

Het ontbreken van een missie en visie over veiligheid op strategisch niveau betekent daarom ook dat er geen sprake is van doorvertaling hiervan naar meetbare strategische doelstellingen. Want wat houdt een veilige leer- en werkomgeving in? Deze vraag wordt in de praktijk niet op strategisch niveau beantwoord, maar meer op operationeel niveau (waarover in de volgende paragraaf meer). Het ontbreken van meetbare strategische doelstellingen over veiligheid heeft ook gevolgen voor de mate en effectiviteit van verantwoording bottom-up (paragraaf 2.3.3) en toezicht (paragraaf 2.3.4).

Verschillen in de governance van 'veiligheid'

Zoals hierboven vermeld, zijn er verschillen tussen de governance van veiligheid bij instellingen waarneembaar. Er is wel één algemene deler te herleiden als het om de governance en invulling van veiligheid gaat. De instellingen hebben veelal veiligheidsbeleid dat gericht is op safety. Het gaat hier om de klassieke maatregelen ten aanzien van het voorkomen en bestrijden van incidenten die dagelijks kunnen voor- komen (brand, ongevallen, inbraak etc.).

⁴ PIOFAH staat voor Personeel, Informatievoorziening, Organisatie, Financiën, Automatisering/Administratie en Huisvesting.

"De noodzaak tot het organiseren van de veiligheid wordt ingegeven door het wettelijk kader enerzijds en de maatschappelijke verantwoordelijkheid anderzijds. Het wettelijk kader voor een veilig gebouw, als externe actor, is te herleiden tot regelgeving vanuit de gebruiksvergunning en de Arbowetgeving."

"Het doel van het IVB-beleid is de adequate bescherming van mensen en middelen. In verhouding tot de directe omgeving moeten de gebouwen en terreinen veiliger zijn, zodat dit verschil in beleving bijdraagt aan het veiligheidsgevoel. De instelling voldoet minimaal aan de wettelijke eisen voor de veiligheid en beveiliging zoals voorgeschreven in de Arbowet, de Archiefwet, Wet op de bescherming persoonsgegevens het Bouwbesluit. Indien geen wettelijk kader wordt gehouden aan de door overheidsinstanties gestelde normen en richtlijnen"

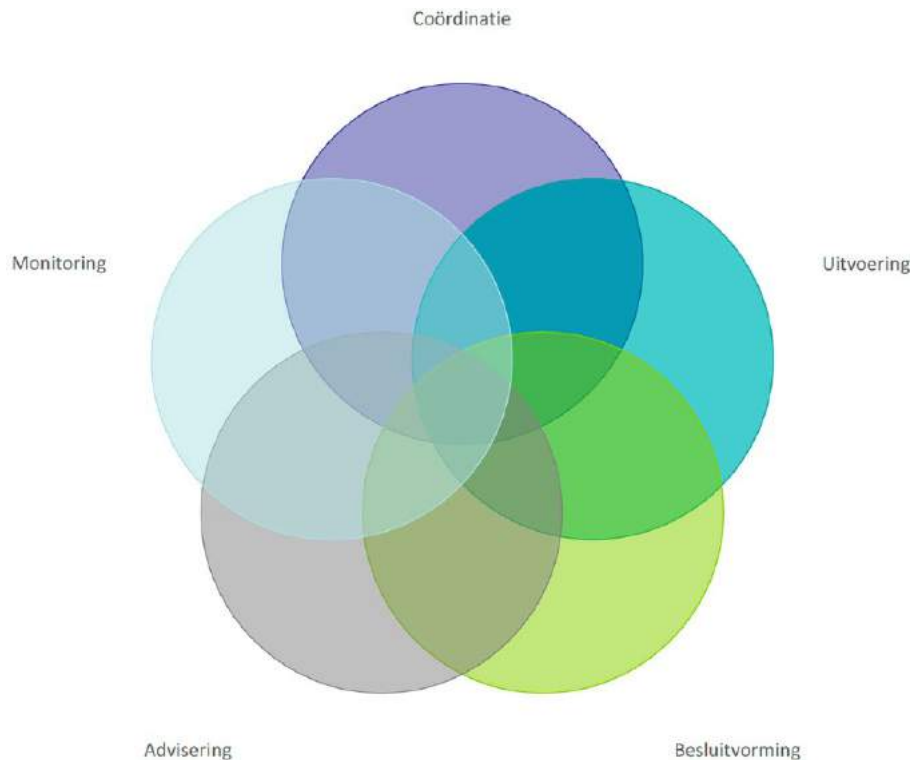
Binnen de scope van safety als leidend principe voor veiligheid constateren wij de volgende verbijzonderingen in de organisatie van veiligheid:

- Organisatie vanuit crisismanagement. Sommige instellingen hebben hun veiligheidsorganisatie en –beleid voornamelijk ingericht vanuit crisismanagement. Crisismanagement is de fase binnen de veiligheidsketen waarbinnen de calamiteiten, rampen en crises bestreden worden. Crisismanagement is in haar aard responsief. Deze aparte zuil bestaat vaak in de vorm van een crisisorganisatie die incidentgericht werkt en geactiveerd wordt door opschaling nadat een incident heeft plaatsgevonden. Een incident wordt hierbij gezien als een "restrisiko" die als potentiële gebeurtenis werkelijkheid is geworden.
- Organisatie vanuit arboveiligheid en technische veiligheid. Deze vorm van veiligheid is gemeengoed in het onderwijsdomein. Deze aandacht vindt haar oorsprong in wet- en regelgeving en vergunningen.
- De aandacht voor sociale veiligheid. Afhankelijk van de ervaring met sociale veiligheid (bedreigingen, pesten, chanteren, omkopen, fraude) hebben instellingen wel of geen aandacht voor sociale veiligheid. Het aantal en soort incidenten op sociale veiligheid zijn bepalend voor de aandacht binnen een kennisinstelling.

We constateren een groeiende aandacht voor moedwilligheid in en rondom de instelling (security). Moedwilligheid betekent de pogingen van mensen of organisaties om de veiligheid te verstoren. Afhankelijk van het ontstaan van een incident kan een brand een safetyrisico zijn (spontane kortsluiting wat tot gevolg heeft een brand) en/of een securityrisico (bewuste poging van een persoon om brand te stichten). Voorbeelden van moedwilligheid zijn: fraude, bedreigingen, aanslagen door gebruik van kennis en middelen van de instelling.

2.3.2 Tactisch / operationeel niveau

Als we inzoomen op de tweede categorie van het governancemodel, het tactisch/operationeel niveau, dan constateren wij vijf rollen. Met rollen bedoelen wij het karakter van de verschillende functiegroepen. Een bepaalde functionaris kan bijvoorbeeld alleen een adviserende rol hebben in de organisatie. Andersom kan ook: de adviserende rol is belegd bij verschillende functionarissen. De rollen die we hierna gaan bespreken zijn bij alle onderzochte instellingen aanwezig. Een rol kan ook door een gremium (een overleg/samenwerkingsverband) vervuld worden bijvoorbeeld het MT of een veiligheidsoverleg.



Figuur 4. Hoofdstructuur governance

De coördinerende rol. De coördinerende rol gaat over de verantwoordelijkheid om de algehele uitvoering van veiligheidsmaatregelen in hun samenhang vorm te geven en uit te zetten binnen de organisatie. Deze rol is tevens een bewakende rol. Het bewaken van de naleving van de afspraken. Voorbeelden van functionarissen zijn: veiligheidsfunctionaris, kwaliteitsmedewerker, directeur bedrijfsvoering of een veiligheidsoverleg.

Uitvoerende rol. Onder deze rol wordt verstaan de verantwoordelijkheid om een veiligheidsmaatregel (of een deel ervan) conform vastgestelde richtlijnen uit te voeren binnen een bepaald termijn. Voorbeelden van functionarissen zijn: veiligheidsfunctionaris, kwaliteitsmedewerker, HRM-medewerker, labbeheerder.

Besluitvormende rol. Onder deze rol wordt verstaan functionarissen die een verantwoordelijkheid hebben ten aanzien van de besluitvorming (strategisch en operationeel) over een veiligheidsmaatregel. Voorbeelden van functionarissen zijn: portefeuillehouder veiligheid CvB, directeuren van faculteiten, managers van faculteiten (indien die aanwezig zijn naast de directeur van een faculteit), veiligheidsoverleg.

Adviserende rol. Onder deze rol wordt verstaan die functionarissen die een adviserende rol hebben richting primair verantwoordelijken ten aanzien van de implementatie van veiligheidsmaatregelen. Deze rol gaat vaak samen gepaard met de coördinerende rol. Voorbeelden van functionarissen zijn: veiligheidsfunctionaris, kwaliteitsmedewerker, directeur bedrijfsvoering, veiligheidsoverleg, HRM-medewerker.

Monitorende rol. De monitorende rol betreft het bewaken van de voortgang van implementatie van veiligheidsmaatregelen. De monitorende rol heeft geen bevoegdheden om implementatie 'af te dwingen'. Via informatieproducten (periodieke rapportages, gesprekken met functionarissen die verantwoordelijk zijn voor implementatie) worden deze functionarissen op de hoogte gehouden van de voortgang van veiligheidsmaatregelen. Voorbeelden van functionarissen zijn: veiligheidsfunctionaris, kwaliteitsmedewerker en directeur bedrijfsvoering.

De onderzochte kennisinstellingen vertonen verschillen ten aanzien van de positionering van de vijf rollen. Zo kan een functionaris meerdere rollen uitoefenen. Aan de andere kant kan een bepaalde rol bij verschillende functionarissen belegd zijn.



Figuur 6. Verschillen positionering van vijf rollen

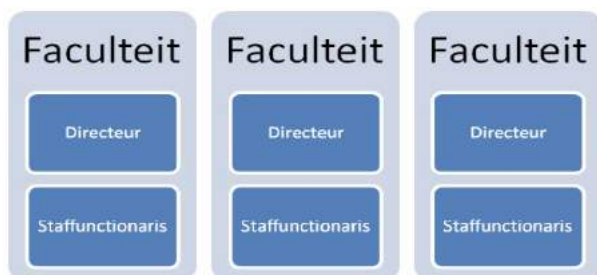
Afstemming en overleg op tactisch/operationeel niveau

Binnen de instellingen zijn naast rollen en functionarissen ook overleggrems aanwezig ten aanzien van het onderwerp veiligheid. Het doel van deze overleggrems is om afstemming te realiseren ten aanzien van de implementatie van veiligheidsmaatregelen en de voortgang te bewaken⁵.

Dit onderzoek laat de volgende vier varianten zien:

Mono-facultair

Een overlegvorm tussen een directeur van een faculteit en een staffunctionaris van de eenheid zelf (lees: veiligheidsfunctionaris). Dit is een mono-facultair overleg waarin alle veiligheidszaken aan bod komen van een faculteit.

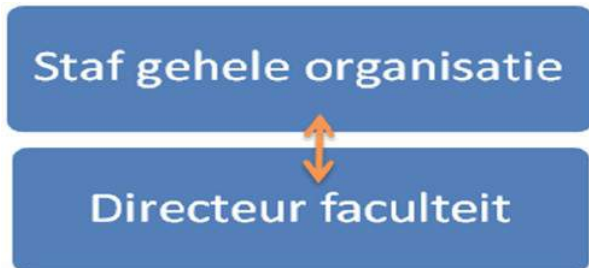


Figuur 7. Mono-facultair

⁵ In sommige overleggrems wordt ook verantwoording afgelegd. Dit komt in de volgende paragraaf aan bod.

Staf-facultair

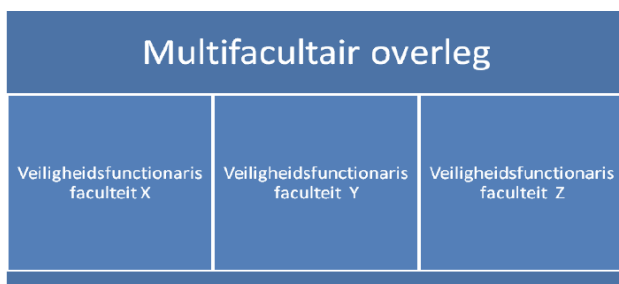
Een overlegvorm tussen een directeur van een faculteit en een staffunctionaris van de complete organisatie. Dit is een overlegvorm waarin afstemming plaatsvindt tussen de veiligheidsmaatregelen van een faculteit en een staffunctionaris van de gehele organisatie. De bespreekpunten blijven in deze variant alleen de mono-facultaire veiligheidsmaatregelen.



Figuur 8. Staf-facultair

Multi-facultair

Een overkoepelende overlegvorm met de veiligheidsfunctionarissen van alle faculteiten, eventueel onder voorzitterschap directeur bedrijfsvoering van een kennisinstelling. Dit betreft een overlegvorm die multi-facultair van aard is. De staffunctionarissen van alle faculteiten die belast zijn met veiligheid, voeren periodiek overleg over keuzes, maatregelen en voortgang. De aard van deze overlegvorm is operationeel van aard.



Figuur 9. Multi-facultair

Interfacultair

Een overkoepelende overlegvorm (meestal in de vorm van een MT-vergadering) met de directeuren van alle faculteiten. Naast een operationeel overkoepelende overlegvorm tussen staffunctionarissen, onderkennen wij ook een overlegvorm van meer strategische aard. Het onderwerp veiligheid is dan –afhankelijk van urgentie van dit onderwerp- een agendapunt tijdens de reguliere MT-vergaderingen tussen de directeuren van de faculteiten.



Figuur 10. Interfacultair

Net als bij de diversiteit van de vijf rollen, constateren wij verschillen tussen de instellingen voor wat betreft de afstemming en het overleg op operationeel niveau. Afhankelijk van factoren als het organisatiemodel, het sturingsmodel en de cultuur, heeft een kennisinstelling één of meerdere gremia voor overleg en afstemming.

Verantwoordelijkheden en bevoegdheden

De verantwoordelijkheden en bevoegdheden ten aanzien van veiligheid binnen de kennisinstellingen zijn het resultaat van de rollen (coördinatie, advisering, uitvoering, besluitvorming, monitoring). Dit onderzoek laat zien dat de rollen verder toegespitst kunnen worden naar de belangrijkste functiegroepen binnen een kennisinstelling.

	CVB	Staf gehele organisatie	Directeur	faculteit	Staf faculteit
Coördinatie		X			
Advisering		X			
Uitvoering		X			X
Besluitvorming	X		X		
Monitoring		X			X

Tabel 1. Koppeling vijf rollen aan functiegroepen

Als we inzoomen op deze vier functiegroepen dan zien we verschillende verantwoordelijkheden en bevoegdheden.

College van Bestuur

Het merendeel van de Colleges van Bestuur –en specifiek de portefeuillehouder veiligheid– heeft voornamelijk een besluitvormende rol. Vanuit hun hoedanigheid en verantwoordelijkheden, worden er op dit niveau besluiten genomen die de gehele organisatie raken, ook voor veiligheid. Besluitvorming over veiligheidsmaatregelen die alleen één of een deel van de faculteiten raken, vindt over het algemeen niet op het niveau van CvB plaats. De portefeuillehouder veiligheid van het CvB wordt hierbij met name geïnformeerd door de directeur bedrijfsvoering van de gehele organisatie.

Staf gehele organisatie

De staforganisatie van de gehele organisatie heeft - afhankelijk van de instelling- alle rollen, behalve besluitvorming. Dat past ook in het reguliere governance-model, waarin deze rollen zijn toebedeeld aan de staforganisatie.

Decaan/Directeur

De decanen of directeuren van de faculteiten (beheerseenheden) vervullen met name een besluitvormende rol. In hun hoedanigheid als decaan/directeur van een faculteit met dito budgetverantwoordelijk, nemen zij besluiten ten aanzien van veiligheid die specifiek voor hun faculteit gelden. De decaan/directeur van een faculteit neemt een belangrijke positie in ten aanzien van veiligheid. Dit ligt in het verlengde van de verantwoordelijkheid voor de drie hoofdprocessen binnen een faculteit, te weten onderwijs, onderzoek en ondersteuning. Er bestaat een grote mate van autonomie van de directeuren om een koers te bepalen ten aanzien van het gewenste veiligheidsniveau. Deze autonomie is het gevolg van drie factoren:

- De juridische autonomie die belegd is in instellingsbesluiten van een instelling;
- De financiële autonomie vanwege de verantwoordelijkheid als budgethouder;

- De informele autonomie vanwege hun positie (gezag) binnen een kennisinstelling. Van oudsher zijn decanen/directeuren van faculteiten (ex-) hoogleraren/docenten die in hun carrière ook managementverantwoordelijkheden hebben gekregen. Het is dan ook niet verwonderlijk dat de eerste aandacht uitgaat naar onderwijs en onderzoek.

Staf-faculteit

Staffunctionarissen van een faculteit vervullen, afhankelijk van de organisatie-inrichting, vooral een operationele en een monitorende rol. Deze rollen vinden hun basis in de PIOFAH-bedrijfsprocessen.

Doorvertaling veiligheid naar primaire processen

Als gevolg van de verschillende rollen en de verschillende posities van de belangrijkste stakeholders binnen een kennisinstelling constateren wij een omgeving waarin er sprake is van een geringe doorvertaling van veiligheid naar primaire processen (onderwijs en onderzoek). Dit is het gevolg van de volgende factoren:

- Decanen/Directeuren van faculteiten leggen hun prioriteiten eerder bij onderwijs en onderzoek dan bij veiligheid.
- Veiligheid binnen kennisinstellingen in het algemeen en faculteiten in het bijzonder heeft voornamelijk een safety-achtergrond en minder security, of andere integrale veiligheid issues. Dit zien we met name bij risico-inventarisaties.
- Ten aanzien van veiligheid gaat de aandacht eerder uit naar het minimaal voldoen aan wet- en regelgeving. Aanvullende veiligheidszaken, zoals sociale veiligheid, moedwilligheid, fraude, hebben gezien de mindere externe druk over het algemeen ook minder aandacht.
- Decanen/Directeuren van faculteiten leggen nog onvoldoende zelf de link tussen het nut (de mogelijke kansen zoals concurrentievoordeel) en de noodzaak van safety en security voor de continuïteit en populariteit (vertaald in aanwas studenten) en bekendheid/kwaliteit (vertaald in aanwas 3e geldstroom). Signalen die bottom-up aan de orde komen worden mede hierdoor onvoldoende opgepakt op strategisch facultair niveau.
- De invulling van taken en bevoegdheden wordt vooral top down geregisseerd en is heel sterk financieel (budget) gestuurd. Prioriteiten ten aanzien van veiligheid worden veelal voor de korte termijn bepaald.

Instrumenten en maatregelen

De onderzochte kennisinstellingen tonen een grote variëteit aan instrumenten en maatregelen om de veiligheid te borgen (voorkomen, bestrijden en nazorg). Hieronder is een opsomming van de instrumenten en maatregelen die over het algemeen bij elke kennisinstelling aanwezig is.

- Bedrijfshulpverlening (BHV). BHV is de hulp die wordt verleend bij ongewenste gebeurtenissen, zoals brand en ongevallen, in een organisatie, die de veiligheid en/of gezondheid van de werknemers en andere aanwezigen bedreigen.
- Brandveiligheid. Er zijn diverse wetten, regels en afspraken over brandveiligheid. Belangrijkste wet is het Gebruiksbesluit van 2008. Dit is een landelijk uniforme regeling voor het brandveilig gebruiken van gebouwen.
- ICT. De beveiliging van de basis ICT-infrastructuur door afstemming en acceptatie op gebruikersniveau. Dit omvat een groot aantal andere aspecten: technisch, organisatorisch, fysiek en procedureel.
- Toegangscontrolesystemen. Het doel is het beperken van de toegankelijkheid van een terrein, een gebouw of een ruimte.

- Cameratoezicht. Het houden van toezicht op een gebouw, gebied of (groepen) mensen met behulp van bewakingscamera's. De twee belangrijkste doelen van cameratoezicht op openbare plaatsen zijn a) het terugdringen van overlast en criminaliteit en b) het vergroten de veiligheidsbeleving.
- Maatregelen op basis van een risicoanalyse, RI&E. Binnen alle onderzochte kennisinstellingen vinden periodieke audits plaats in de vorm van RI&E's (risico-inventarisatie en evaluatie). De RI&E's zijn een verplichting vanuit de Arbeidsomstandighedenwet. Dit betekent dat de onderzochte RI&E's het karakter hebben van veilig en gezond werken. Het gaat dan om de veiligheid van medewerkers, studenten en derden.
- Crisismanagement. Onder crisismanagement verstaan we het geheel aan organisatorische, procedurele en materiële voorzieningen met als doel de organisatie voor te bereiden op crises, deze zo mogelijk te voorkomen en, bij het manifest worden van een crisis, de gevolgen ervan te beheersen.
- Bedrijfsnoodplannen. In een bedrijfsnoodplan zijn de preventieve en repressieve maatregelen vastgelegd die een organisatie heeft genomen om in het geval dat, de continuering van de bedrijfsvoering en de veiligheid van het personeel in gevaar dreigt te komen een optreden van de bedrijfshulpverleningsorganisatie gewaarborgd is. Voorbeelden hiervan zijn een ontruimingsplan en een ICT-back-up systeem.
- Maatregelen op basis van incidentenregistratiesystemen. Dit zijn systemen waarin incidenten geregistreerd worden ten behoeve van beleidsvorming, monitoring en/of navolging (actie).

2.3.3 Verantwoording

De derde categorie binnen het governance toetsingskader is de mate van verantwoording bottom-up door middel van informatieproducten (rapportages, beoordelingsgesprekken). We maken een onderscheid tussen verantwoording op strategisch en operationeel niveau.

Naleving strategische doelen

Strategische verantwoording is de verantwoording door relevante functionarissen over de strategische doelstellingen ten aanzien van veiligheid. In paragraaf 2.3.1 (strategisch niveau) hebben we reeds beschreven dat de afwezigheid van een visie op strategisch niveau met zich meebrengt dat ook de doorvertaling van veiligheid op strategisch niveau ontbreekt. Het gevolg hiervan is dat er daarom ook geen verantwoording kan plaatsvinden over strategische doelstellingen. Dit onderzoek bevestigt dit ook. De afwezigheid van strategische verantwoording wordt ook versterkt door het feit dat veiligheid onvoldoende onderdeel is van een algeheel PDCA-cyclus. Indien we inzoomen op de strategische verantwoording door de decanen/directeuren van de faculteiten, dan constateren wij dat op een uitzondering na, veiligheid geen onderdeel is van hun functionerings- en beoordelingsgesprekken.

De directeuren/decanen worden tot op de dag van vandaag voornamelijk beoordeeld door CvB op hun onderwijs- en onderzoeksdoelstellingen. Dit geldt ook voor de verantwoording van het CvB aan de Raad van Toezicht. Dit onderzoek laat zien dat de Raad van Toezicht geen toezicht uitoefent op strategisch niveau van het veiligheidsbeleid. Ook bij de Raad van Bestuur staan de onderwijs- en onderzoeksdoelstellingen centraal in de beoordelingssystematiek.

Naleving operationele doelen

Operationele verantwoording is de verantwoording door relevante functionarissen over de operationele doelstellingen ten aanzien van veiligheid. Op operationeel niveau vindt op verschillende niveaus door middel van verschillende informatieproducten verantwoording plaats:

- Verantwoording door staffunctionaris van een faculteit aan directeur van faculteit (voortgangsrapporten en functionerings- en beoordelingsgesprekken). Dit in het geval de staffunctionaris niet gedetacheerd is vanuit een centrale stafafdeling, maar hiërarchisch onder de decaan/directeur van een faculteit valt.
- Verantwoording door staffunctionaris van een faculteit aan directeur van centrale stafafdeling. Dit in het geval de staffunctionaris gedetacheerd is vanuit de centrale stafafdeling.
- Verantwoording door decaan/directeur faculteit aan MT (voortgangsrapporten)
- Verantwoording van decaan/directeur faculteit aan directeur bedrijfsvoering organisatiebreed (voortgangsrapporten)
- Verantwoording van directeur bedrijfsvoering organisatiebreed aan CvB (voortgangsrapporten en functionerings- en beoordelingsgesprekken)

Opmerkingen ten aanzien van operationele verantwoording

- Over het algemeen vindt de borging en verantwoording niet plaats aan de hand van SMART-eisen
- We zien grote verschillen in de wijze waarop incidenten door instellingen worden geregistreerd en gerapporteerd.
- De wijze waarop incidenten worden geregistreerd en of er al dan niet een integrale analyse op plaatsvindt verschilt per instelling. Gesignaleerde incidenten worden meestal op niveau eigen faculteit opgelost.
- Geen van de instellingen kiest ervoor om over de analyse/audit of overige prestatie indicatoren op het gebied van veiligheid informatie te publiceren in jaarverslagen of andere media.
- Verantwoordelijkheid voor het vraagstuk security (hoe om te gaan met moedwillige scenario's) ligt vooral bij staforganisatie organisatiebreed en niet bij de faculteiten.

2.3.4 Toezicht

De vierde categorie binnen het governance toetsingskader is de mate van (effectief) toezicht op het veiligheidsbeleid en -organisatie van een kennisinstelling. Er is een onderscheid tussen intern en extern toezicht die voor alle onderzochte kennisinstellingen geldt.

Intern toezicht

RI&E's

De periodieke RI&E's geven inzicht in het risiconiveau van de organisatie en de wenselijke aanvullende maatregelen. Tot op heden vindt er alleen toezicht plaats op het verrichten van de RI&E's. Er vindt nagenoeg geen toezicht intern plaats op de aanvullende maatregelen op basis van de risicoanalyse.

Fragmentatie

Interne audits worden niet integraal uitgevoerd, maar gefragmenteerd. Dit geldt ook voor interne audits waarin veiligheid een deelonderwerp is. Denk aan de verschillende audits ten aanzien van medewerkersveiligheid, technische veiligheid en informatieveiligheid. Toezicht in de vorm van interne audits kunnen uitgevoerd worden door een sectie integrale veiligheid of door een College van bestuur. In enkele instellingen zien we deze structuur in ontwikkeling.

Raad van Toezicht

De Raad van Toezicht is belast met het toezicht op het bestuur en beheer van de gehele organisatie. Het College van Bestuur legt verantwoording af aan de Raad van Toezicht. Hoewel de Raad van Toezicht een formeel orgaan is die bij wet is vastgelegd, constateren wij de Raden van Toezicht (zoals eerder opgemerkt in dit hoofdstuk) geen aandacht besteden aan de naleving van veiligheidsdoelen op strategisch niveau. Dit komt zoals gezegd door de primaire aandacht voor de onderzoeks- en onderwijskwaliteit.

Extern toezicht

Wettelijk toezicht

Extern toezicht vindt plaats door organisaties die vanuit hun wettelijke verantwoordelijkheid als vergunningverlener extern toezicht uitoefenen. Het gaat dan om de volgende toezichthouders:

- Gemeente
- Brandweer
- Bouw- en woningtoezicht
- Inspectie nationale overheid, waaronder:
 - o Arbeidsinspectie
 - o Inspectie Openbare Orde en Veiligheid
 - o Kernfysische dienst Ministerie van IenM
 - o Onderwijsinspectie en ministerie van OCW (accreditatie)
 - o Voedsel- en Warenautoriteit

Vrijwillig extern 'toezicht'

Soms wordt een extern bureau ingehuurd, maar dan meestal voor toezicht op de crisisorganisatie van een kennisinstelling.

2.4 Mogelijke verklaringen voor huidige governance en bedrijfsvoering van integrale veiligheid

Kennisinstellingen zijn van nature omgevingen waarin openheid, toegankelijkheid en transparantie belangrijke kernwaarden zijn. Deze kernwaarden garanderen een omgeving voor het bieden en volgen van kwalitatief goed onderwijs. Onderzoek en onderwijs zijn derhalve de primaire bestaansgronden voor een universiteit en een hogeschool.

Risico's die deze bestaansgronden bedreigen (verlies van kwaliteit van onderwijs, onderzoek, imagoschade) krijgen van nature veel aandacht. Dit heeft zich in de loop van de tijd vertaald in een governance-model voor onderzoek en onderwijs. Onderzoek en onderwijs worden vanuit de optiek van bedrijfsvoering gezien als primaire processen. Secundaire processen zoals PIOFAH bieden een organisatie-omgeving om de bestaansgronden (onderzoek en onderwijs) te garanderen.

Veiligheid is van oudsher een secundair proces binnen een kennisinstelling. Dat is niet zo verwonderlijk aangezien kennisontwikkeling en kennisdeling het bestaansdoel zijn van een kennisinstelling. Echter, de laatste decennia is door de toename van het aantal veiligheidsincidenten, de media- en politieke aandacht daarvoor en de mondigheid van de burger (studenten en ouders) een verschuiving ontstaan in dit paradigma. Het gebrek aan veiligheid wordt steeds breder onderkend als serieus risico voor de continuïteit van de kennisinstellingen.

De huidige 'onderwaardering' van veiligheid is mede het gevolg van de cultuur binnen het onderwijsdomein waarbinnen faculteitsdecanen/directeuren, leden van CvB én Raad van Toezicht ex-hoogleraren c.q. ex-docenten zijn die zich ontwikkeld hebben tot manager. Vanwege deze achtergrond van de bestuurders en het management wordt de kwaliteit van de organisatie van nature afgemeten aan onderzoek en onderwijs en minder aan veiligheidsrisico's. Dit wordt nog eens versterkt door de formele (middels budgetverantwoordelijkheid) en informele (status van faculteitsdecanen/directeuren) positie van faculteiten binnen universiteiten en hogescholen. Het is ons opgevallen dat er voor deze verklaringen geen noemenswaardige verschillen zijn tussen universiteiten (met onderzoek) en hogescholen (zonder onderzoek). Bij zowel universiteiten als hogescholen bestaat de traditie om de functies binnen het bestuur en faculteitsmanagement te laten vervullen door ex-hoogleraren en ex-docenten. We zien wel bij sommige kennisinstellingen pogingen om deze traditie te doorbreken door managers van buiten de organisatie met een niet-onderwijs achtergrond te benoemen.⁷

Deze factoren gezamenlijk bepalen de scope voor veiligheid in het onderwijs- en onderzoeksdomein. Op basis van de bevindingen, overeenkomsten, verschillen en best-practises, kan een voorstel gemaakt worden voor een blauwdruk voor de governance van integrale veiligheid. Dit komt in hoofdstuk drie aan bod.

Op dit moment heeft u twee bouwstenen behandeld. Daarmee heeft u inzicht gekregen in de achterliggende theorie en heeft u kunnen lezen over de huidige praktijk van governance en bedrijfsvoering van integrale veiligheid binnen universiteiten en hogescholen. Herkent u binnen uw organisatie een van de beschreven governance modellen? Zijn er bepaalde sturingselementen die ook op uw organisatie van toepassing zijn?

De 2e bouwsteen is erop gericht u als lezer inzicht te geven in het governancemodel hoger onderwijs en de verschillende manieren waarop universiteiten en hogescholen de veiligheidsfunctie op dit moment binnen de governance en bedrijfsvoering hebben belegd. Voordat u zich richt op bouwstenen 3 en 4 uit het tweede deel, de implementatie van integrale veiligheid, is het raadzaam om eerst ook voor uw eigen organisatie de IST-situatie te bepalen.

⁶ Deze traditie zien we ook terug in andere domeinen zoals ziekenhuizen, rechtbanken en arrondissementsparketten (OM). In deze domeinen zijn de bestuurders en budgethouders afkomstig vanuit dezelfde organisatie (specialisten bij ziekenhuizen, rechters bij rechtbanken en officieren van justitie bij OM).

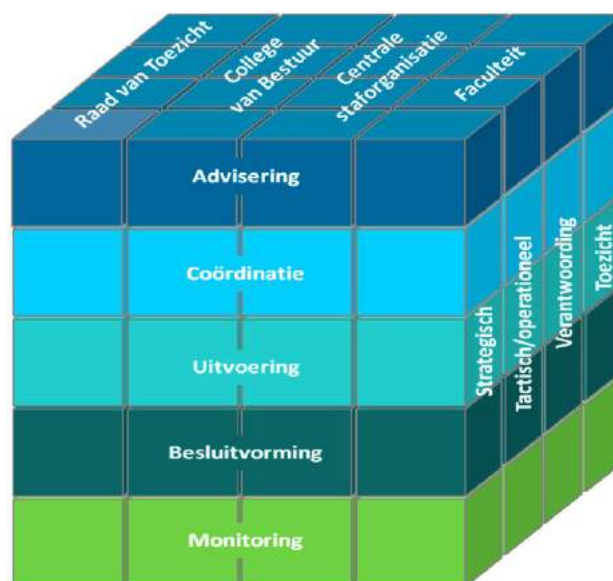
Deel II: Implementatiehandleiding met stappenplan

Blauwdruk voor integrale veiligheid in de governance en bedrijfsvoering



3.1 Inleiding

Het voorgaande hoofdstuk leert dat op basis van het governance toetsingskader een invulling gegeven moet worden aan de elementen uit een driedimensionale matrix. In deze matrix worden de vier categorieën van de governance structuur gecombineerd met de verschillende rollen en functionele groepen in de organisatie.



Figuur 11: Driedimensionale governance matrix

In dit hoofdstuk beschrijven wij op basis van deze matrix twee blauwdrukken voor het implementeren van integrale veiligheid (IV) binnen het hoger onderwijs.

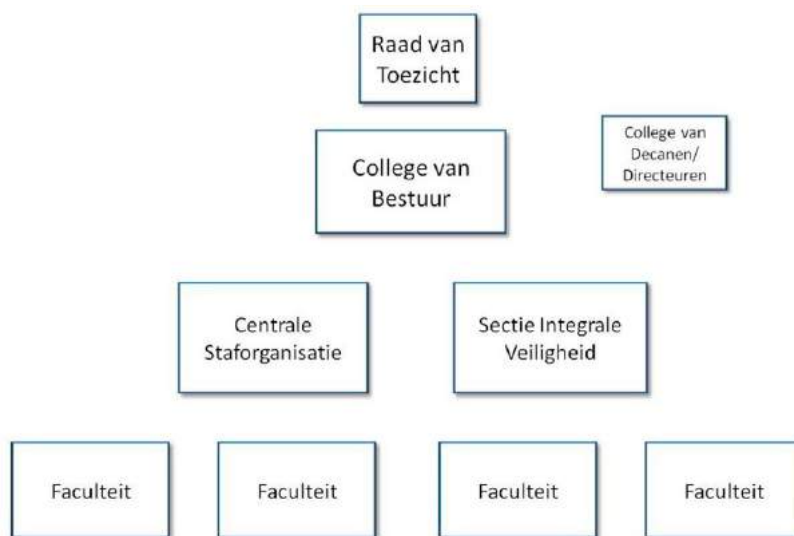
Dit hoofdstuk (en ook hoofdstuk 4) wijkt af van de vorm van hoofdstuk 2. Hoofdstuk 2 is een weergave van de analyse van het onderzoek en is daarom een inhoudelijk hoofdstuk. Hoofdstuk 3 heeft een andere vorm en richt zich op de blauwdruk. Vandaar ook dat in dit hoofdstuk per rol een uitwerking plaatsvindt door middel van figuren.

Dit hoofdstuk is als volgt opgebouwd. De eerste blauwdruk (paragrafen 3.2 en 3.3) richt zich op de governance van IV; een aansturingsmodel op strategisch, tactisch operationeel niveau. De tweede blauwdruk (paragraaf 3.4) beschrijft vervolgens de processen die in de bedrijfsvoering van de organisaties moeten worden doorgevoerd om integrale veiligheid te kunnen sturen en te beheersen.

3.2 Governance van Integrale Veiligheid (Soll- model)

In hoofdstuk twee beschreven we vijf rollen die binnen een instelling of organisatie op de juiste manier belegd moeten worden om IV op tactisch/operationeel niveau te kunnen realiseren. We constateerden dat al deze rollen vanuit een veiligheidsaspect wel degelijk binnen de onderzochte instellingen aanwezig zijn, maar dat de samenhang en de aansturing ervan ontbreekt. Ook constateerden we dat de rollen niet of zelden in logisch verband staan met het algemene governancemodel van de instelling: IST-situatie.

Deze paragraaf geeft in een blauwdruk weer hoe de vijf rollen op het thema integrale veiligheid binnen het algemene governancemodel van de instelling kunnen worden belegd, zodanig dat ze elkaar versterken en er een bestuurlijk optimum gecreëerd wordt.



Figuur 12. Overzicht organisatie-entiteiten voor governance integrale veiligheid

Strategisch, tactisch en operationeel

De wijze waarop de vijf verschillende rollen binnen het bestaande governancemodel kunnen worden belegd wordt steeds per rol toegelicht met een organogram. De organogrammen zijn opgebouwd uit drie lagen: een strategische laag, een tactische laag en een operationele laag. De strategische laag bestaat uit: De Raad van Toezicht, het College van Bestuur en het College van Decanen (universiteit) of het College van Directeuren (hogescholen). De tactische laag bestaat uit ondersteunende diensten en de Sectie Integrale Veiligheid. Op operationeel niveau zijn de faculteiten geplaatst die ten aanzien van IV vooral een operationele rol te vervullen hebben.

Het Soll – governance model

De verschillende entiteiten die het bestuurslandschap van een hogeschool of universiteit vormen hebben elk één of meerdere rollen te vervullen. De vijf rollen zoals in deze handleiding onderscheiden worden in de 'SOLL' situatie als volgt door de verschillende entiteiten ingevuld.

SOLL-model:	RvT	CVB	Centrale Stafororganisatie	Centrale staf sectie IV	College Decanen	Staf faculteit
Coördinatie		X	X	X	X	X
Advisering		X	X	X	X	X
Uitvoering			X			X
Besluitvorming		X	X	X		X
Monitoring	X	X	X	X		X

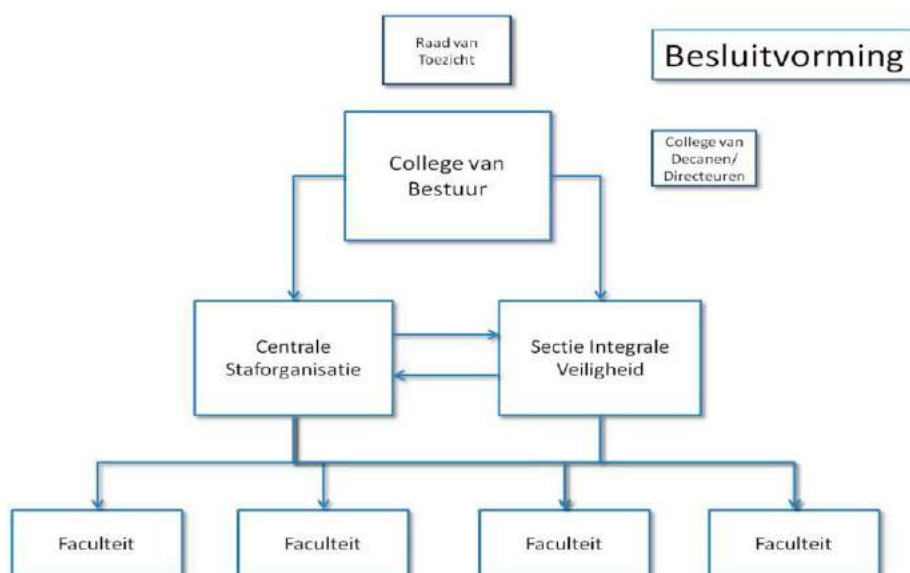
Tabel 2. Samenvatting van het Soll-governance model

3.3 Rollen in de Soll- Situatie

Elke entiteit (in deze handleiding eerder functiegroep of organisatieonderdeel genoemd) heeft één of meerdere rollen. Het belang van het organisatie- onderdeel ten aanzien van de invulling van de rol kan verschillen. Dit verschil wordt in de modellen in deze paragraaf per rol visueel uitgedrukt in de grootte van het blok, zo is bijvoorbeeld de rol van de faculteiten bij uitvoering (operationeel) veel groter dan bij het besluitvormingsproces. De blokken van de faculteiten zijn bij uitvoering groter afgebeeld dan de andere blokken. Bij besluitvorming zijn het CvB en de Centrale Stafororganisatie van belang, de hogere echelons, zowel strategisch als tactisch. De blauwe blokken van deze organisatieonderdelen zijn daarom groter afgebeeld dan die van de faculteiten.

3.3.1 Besluitvorming

In deze deelparagraaf is de rol besluitvorming uitgewerkt over de organisatie-entiteiten. De lijnen in onderstaand figuur geven weer welke entiteiten een besluitvormingsrol hebben en hoe de aansturing van de besluit- vorming dient plaats te vinden.



Figuur 13. Governance van besluitvorming voor integrale veiligheid

Strategisch niveau

Het strategisch niveau is het fundament van de governance van IV. Op strategisch niveau is het College van Bestuur hét orgaan om de visie, missie en strategische doelstellingen te formuleren. Want wat betekent het om een veilige leer- en werkomgeving te zijn. In een CvB zal de portefeuillehouder hier primair voor verantwoordelijk zijn. Hij bewaakt de doorvertaling van de strategische doelstellingen door middel van jaarplannen (wat zijn de doelstellingen ten aanzien van veiligheid?). Het CvB neemt op strategisch niveau besluiten omtrent de tactische en operationele uitvoering van veiligheid binnen de organisatie. Op strategisch niveau wordt er ook besluiten genomen over:

- Verantwoordelijkheidsverdeling
- Toekennen van budgetten
- Verantwoording van uitgevoerde maatregelen

Tactisch niveau

De centrale staforganisatie krijgt doelstellingen en richtlijnen opgelegd vanuit instellingsbreed beleid (strategie/visie) door het CvB en zet dit om in tactisch en operationele besluiten. Indien er binnen de organisatie tevens een integraal veiligheidsoverleg aanwezig is vindt er afstemming plaats tussen de centrale staforganisatie en de Sectie IV⁸. De centrale staforganisatie en de Sectie Integrale Veiligheid (SIV) nemen hun besluiten op tactisch/ operationeel niveau, stemmen deze onderling af en communiceren dat vervolgens als één beleid richting de faculteiten.

De governance van IV vraagt om een Sectie Integrale Veiligheid op tactisch niveau. Dit onderdeel faciliteert onder andere het Integraal Veiligheidsoverleg dat wordt gevormd door decanen/directeuren of hun secretarissen, management van de ondersteunende diensten en de portefeuillehouder IV van het College van Bestuur.

De Sectie Integrale Veiligheid zet beleid uit op tactisch/operationeel niveau en zorgt voor afstemming op dit thema binnen de instelling.

Operationeel niveau

Het beleid dat op strategisch en tactisch niveau is uitgezet wordt vervolgens op operationeel niveau binnen de faculteiten/clusters doorgevoerd. Besluitvorming binnen de faculteiten/clusters is daarmee zeer praktijkgericht, instellingsspecifiek en ingekaderd door het overkoepelende beleid. Iedere faculteit is zelf verantwoordelijk voor het nemen van veiligheidsmaatregelen op operationeel niveau. Dit in lijn met de besluiten op strategisch en tactisch niveau.

Voordelen van een goede rolverdeling ten aanzien van de besluitvorming over integrale veiligheid:

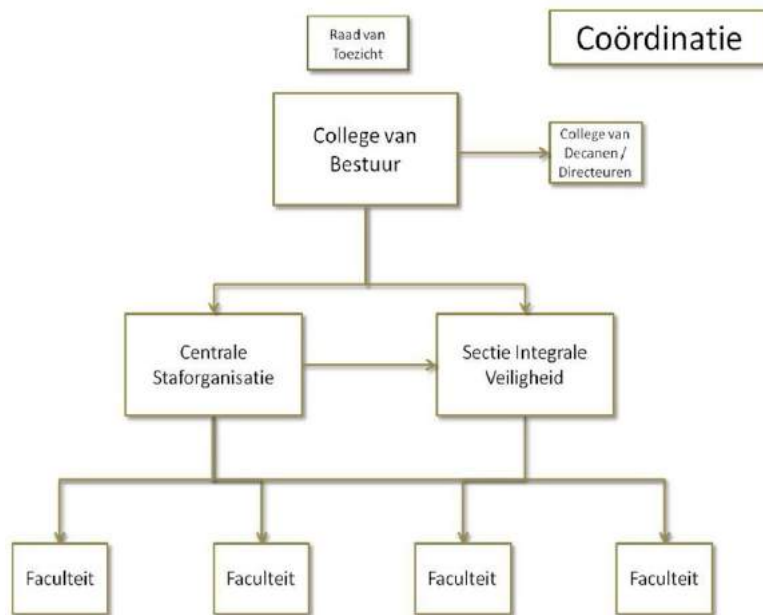
- Helder beleid dat vanuit één instellingsbrede visie wordt vormgegeven
- Betrokkenheid en sponsoring door specifiek benoemde rol ten aanzien van besluitvorming over IV binnen het College van Bestuur
- De doorvertaling van algemeen beleid en visie naar tactisch beleid en tactisch operationele maatregelen versterkt de eenduidigheid in besluitvorming over beleid, bevordert de integrale aanpak en stimuleert de onderlinge afstemming tussen de beslissingsbevoegde organisatieonderdelen

⁸ Het integraal veiligheidsoverleg (gefaciliteerd door de SIV) heeft als rol het organisatorisch en procesmatig functioneren van de centrale staforganisatie te monitoren. Het monitoren is erop gericht om op horizontaal niveau te controleren of de centrale staforganisatie naar behoren haar taak in het samenwerken met, adviseren aan en ondersteunen van de faculteiten kan vormgeven.

- De besluitvormingsrol ten aanzien van IV wordt niet bij het college van decanen of directeuren belegd, zij focussen zich vooral op algemene kwaliteit waarborging (RvT), onderwijs en onderzoek (college van decanen en directeuren)

3.3.2 Coördinatie

In deze deelparagraaf is de rol coördinatie uitgewerkt over de organisatie-entiteiten. De lijnen in onderstaand figuur geven weer welke entiteiten een coördinerende rol hebben en hoe de aansturing van de coördinatie dient plaats te vinden.



Figuur 14. Governance van coördinatie voor integrale veiligheid

Strategisch niveau

Coördinatie van integraal veiligheidsbeleid op strategisch niveau is van groot belang. Het CvB heeft een essentiële rol in het coördineren van de beleidsimplementatie door de verschillende organisatieonderdelen. Het CvB stuurt op de integrale aanpak van veiligheidsvraagstukken zoals deze door haar in het strategisch beleid en de organisatie visie zijn neergelegd. Tijdens overleggen met het college van decanen en directeuren wordt het onderwerp IV een standaard agendapunt. Het college van decanen en directeuren wordt hierdoor geïnspireerd open te staan voor coördinatie vanuit strategisch en tactisch niveau.

Tactisch niveau

De centrale staforganisatie en de SIV worden vanuit strategisch niveau gecoördineerd en aangestuurd door het CvB (in het bijzonder de portefeuillehouder veiligheid). De centrale staforganisatie, onderdeel SIV, coördineert en faciliteert de activiteiten van het integraal veiligheidsoverleg. Het CvB bewaakt (indien aanwezig) ook de coördinatie van het integraal veiligheidsoverleg door lid te zijn van dit overleg. In gezamenlijkheid coördineren de centrale staforganisatie en de SIV vervolgens de tactische keuzes in de uitvoering van het beleid richting de faculteiten.

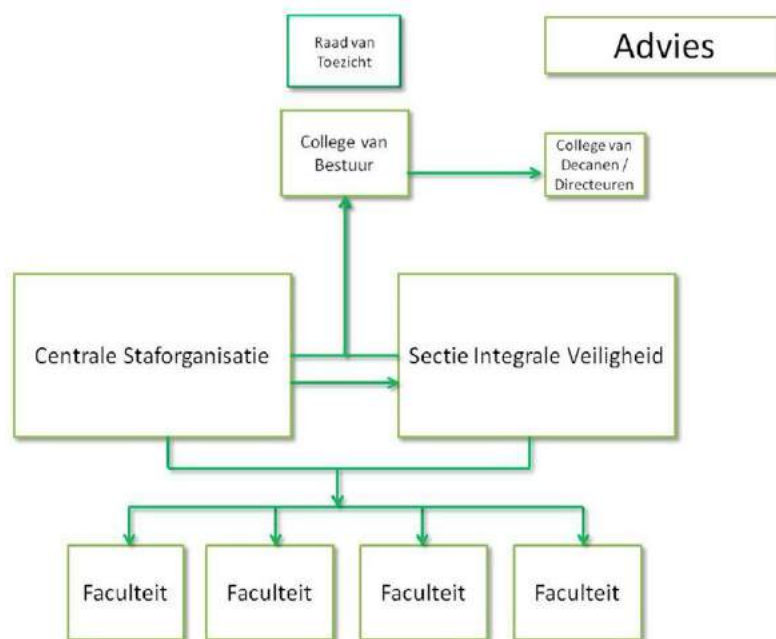
Operationeel niveau

De faculteiten hebben ook een rol ten aanzien van de coördinatie van IV. Hun rol is operationeel uitvoerend van aard. De coördinatie die vereist is op dit niveau heeft betrekking op het agenderen van het onderwerp en het sturen op het behalen van resultaten en het nastreven van de integrale visie ten aanzien van veiligheid binnen de faculteit. De voordelen van een goed georganiseerde coördinatie

- Deze zijn vooral gelegen in het belang van de rol die bij het CvB wordt belegd. Het CvB heeft nu meer dan voorheen een belang bij een goede aansturing/coördinatie van IV. Ze heeft immers zelf het strategisch beleid uitgezet en haar visie bepaald. Zij verplicht zichzelf hiermee om hierop in het jaarverslag terug te komen en de behaalde resultaten te bespreken.
- Het integrale veiligheidsoverleg krijgt een belangrijke functie in de governance van IV binnen de organisatie. Voor het goed functioneren van dit organisatieonderdeel is het noodzakelijk dat de het centrale staforgaan de coördinatie en het faciliteren op zich nemen.

3.3.3 Advies

In deze deelparagraaf is de rol advisering uitgewerkt over de organisatie-entiteiten. De lijnen in onderstaand figuur geven weer welke entiteiten een adviserende rol hebben en hoe de aansturing van de adviseringdient plaats te vinden.



Figuur 15. Governance van advisering voor integrale veiligheid

Strategisch niveau

Het College van Bestuur heeft in dit model een relatief kleine rol ten aanzien van het adviseren over IV. Enkel de portefeuillehouder IV van het college denkt vanuit zijn vaktechnische kennis op strategisch niveau mee. Het actief adviseren richting de faculteiten over specifieke tactische en operationele vraagstukken laat de portefeuillehouder over aan de ondersteunende diensten en de speciaal daarvoor ingestelde SIV. Het CvB heeft wel tot taak de adviesrol van de SIV adviesrol te formaliseren en hierover te communiceren richting de faculteiten.

Tactisch niveau

De blauwdruk voor de rol van adviseur kent een belangrijke taak toe aan de Centrale Staforganisatie en de SIV. Deze twee organisatie- onderdelen hebben van origine een adviserende rol in de richting van de andere entiteiten. Zeker als het gaat om onderwerpen zoals ARBO en fysieke veiligheid dan hebben de ondersteunende diensten nu eenmaal de meeste inhoudelijke kennis en ervaring.

Uit ons deskresearch en de interviews blijkt dat deze rolverdeling in de bestaande governance modellen al zeer gebruikelijk is. Een effectieve invulling van deze rol is echter alleen mogelijk indien voldoende borging van dit advies geregeld is en de adviseur voldoende kwaliteit heeft. De advieslijnen moeten daarom meer geformaliseerd worden en kenbaar gemaakt binnen de gehele organisatie.

De ondersteunende diensten en de SIV brengen advies uit aan het CvB en aan de faculteiten. Er wordt zowel gevraagd (op elk willekeurig moment) als ongevraagd (op vast ingeplande momenten) geadviseerd over alle aspecten rond IV. Alle onderdelen van integraal management komen daarbij aan bod, van het bepalen van de risico's, het inventariseren van geschikte maatregelen en het uitvoeren van veiligheidsbeleid tot en met het meten van prestaties en opstellen van verbeterplannen.

Omdat elke faculteit een unieke risicostructuur en een specifiek daarop afgestemde adviesbehoefte heeft moet met elke faculteit een eigen adviesrelatie worden opgebouwd. Het advies moet zowel een tactische als operationele component bevatten, al naar gelang het onderwerp de behoefte van de faculteit op dat punt.

Operationeel niveau

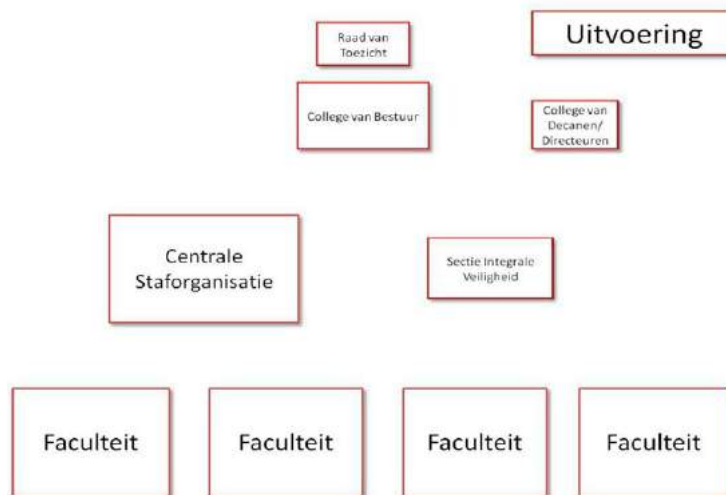
De faculteiten hebben een minimale rol ten aanzien van advisering over IV. Zij worden in hun rol als uitvoeringsverantwoordelijke geadviseerd door de centrale en de SIV. Taak voor de faculteiten is om tijdig om advies te vragen, bijvoorbeeld over hoe de gestelde doelen ten aanzien van IV voor deze specifieke faculteit behaald kunnen worden. Of hoe een specifieke situatie aangepakt moet worden, bv. vandalisme of toenemende onveiligheidsgevoelens bij studenten en medewerkers. Vervolgens is het aan de faculteit om het advies ter harte te nemen en de voorgestelde maatregelen te implementeren.

Voordelen van het benoemen en organisatiebreed beleggen van adviesrollen

- Primaire adviesrol belegd bij onderwerpsdeskundige en verantwoordelijke voor uitvoering.
- Adviesrol op dit specifieke onderwerp weg bij het decanen- en directeurenoverleg waar het nu vaak belegd is. Zij kunnen zich dan primair toeleggen op adviseren over onderwijs en onderzoek.
- Door het stellen van duidelijke doelen (besluitvorming) kan tijdig en gericht advies gevraagd worden bij het nastreven van die doelen. Het advies is daardoor beter afgestemd op de vraag en zal eerder gevraagd en vervolgens ter harte genomen worden. Alle organisatieonderdelen streven dan hetzelfde doel na.

3.3.4 Uitvoering

In deze deelparagraaf is de rol uitvoering uitgewerkt over de organisatie-entiteiten. De entiteiten hebben in tegenstelling tot de andere rollen een zelfstandige rol bij de uitvoering van veiligheidsmaatregelen. In onderstaand figuur is weergegeven welke entiteiten een uitvoerende rol hebben. De lijnen ontbreken in dit figuur omdat de aansturing plaatsvindt door middel van de andere rollen.



Figuur 16. Governance van uitvoering voor integrale veiligheid.

Strategisch, tactisch en operationeel

Elk organisatieonderdeel kent specifieke taken en bevoegdheden die door hun rol in de uitvoering tot stand worden gebracht. De rol uitvoering bevat geen hiërarchie of verband tussen de verschillende organisatieonderdelen. Elk onderdeel voert, inhoudelijk onafhankelijk van elkaar, de specifiek toebedeelde taken uit. Op tactisch niveau is er binnen de centrale staforganisatie, SIV, een functionaris die het overzicht heeft op de uitvoering van de toebedeelde taken. Decentraal in de staf van de faculteiten zijn functionarissen die de onderwerpen van IV, naast andere taken zoals BHV, Arbo etc. in het pakket hebben zitten. Het beleid dat aan die taken ten grondslag ligt is gericht op het bewaken van de continuïteit van de primaire processen binnen de instelling: onderwijs en onderzoek. Om deze continuïteit te waarborgen is een visie ontwikkeld, zijn besluiten genomen en is beleid opgesteld dat de IV van de instelling nastreeft.

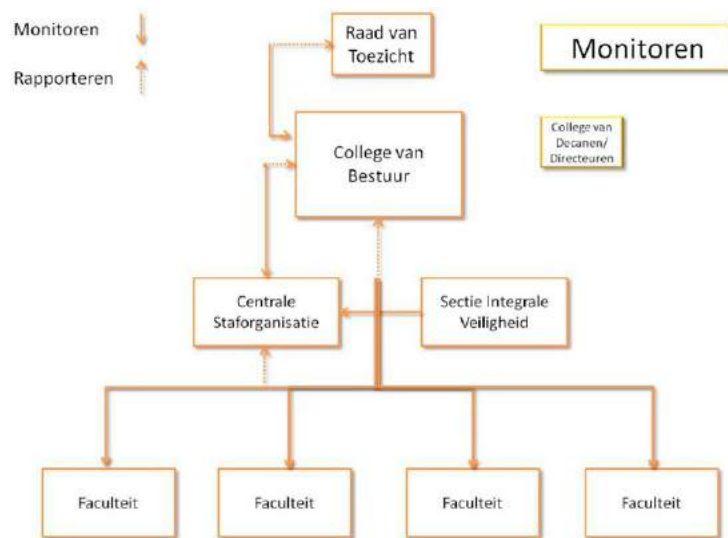
Elk organisatieonderdeel kent haar eigen afgebakende en formeel vastgelegde taken die uitgevoerd moeten worden. Dit maakt sturing op het behalen van resultaten en het tijdig constateren van vraagstukken die om advies of om bijstelling van de doelstellingen vragen eenvoudiger. Doordat elk organisatieonderdeel haar eigen taken uitvoert binnen de visie en het beleid van de hele organisatie wordt een gezamenlijke, organisatiebrede, aanpak van IV tot stand gebracht.

Voordelen van het actief beleggen van taken in de uitvoering van integraal veiligheidsbeleid

- Het biedt een structuur die eenduidigheid van beleid vertaalt naar eenduidigheid in uitvoering
- Het geeft inzicht in de gestelde doelen en de acties die elk organisatieonderdeel op uitvoeringsniveau moet uitvoeren om de gestelde doelen te behalen

3.3.5 Monitoren

In deze deelparagraaf is de rol monitoring uitgewerkt over de organisatie-entiteiten. De lijnen in onderstaande figuur geven weer welke entiteiten een monitorende rol hebben en hoe de aansturing van de monitoring dient plaats te vinden.



Figuur 17. Governance van monitoring voor integrale veiligheid

Strategisch niveau

Het monitoren, of met andere woorden het intern toezicht houden op beleid en het behalen van gestelde doelen, is het sluitstuk van een goed functionerende governancestructuur. Op strategisch niveau voeren de Raad van Toezicht en het College van Bestuur toezicht uit op het nastreven van de visie en de uitvoering van het strategisch beleid. De RvT houdt toezicht op het CvB dat verantwoording aflegt over de prestaties van de universiteit of hogeschool op het gebied van IV.

Het CvB moet monitoren of de gestelde doelen, die op het thema IV zijn benoemd en beschreven, worden behaald. Om de rol van monitoren goed te kunnen uitvoeren wordt het CvB regelmatig geïnformeerd door tactische rapportages vanuit de centrale staforganisatie en/of de SIV. Daarnaast leggen ook de decanen/directeuren zelf verantwoording af over de uitvoering van voorgestelde maatregelen op operationeel niveau. Dit vindt plaats door middel van functionerings- en beoordelingsgesprekken. Door met regelmaat de stand van zaken te beoordelen kan tijdig worden bijgestuurd indien geconstateerd wordt dat de geplande strategische en operationele doelen niet gehaald worden.

Tactisch niveau

Beleid dat op tactisch niveau is opgesteld en de besluiten die zijn gecommuniceerd binnen de organisatie moeten door de centrale staforganisatie worden gemonitord. De centrale staforganisatie houdt daartoe toezicht op de afzonderlijke faculteiten, waarbij het overzicht wordt bewaard op het behalen van zowel de organisatie brede- als de aan de afzonderlijke faculteit specifiek getelde doelen. De centrale staforganisatie rapporteert haar bevindingen inclusief tactisch/operationele oplossingsrichtingen (adviesrol) aan het CvB (portefeuillehouder IV).

Het integraal veiligheidsoverleg (gefaciliteerd door de SIV) heeft als rol het organisatorisch en procesmatig functioneren van de centrale staforganisatie te monitoren. Het monitoren is erop gericht om op horizontaal niveau te controleren of de centrale staforganisatie naar behoren haar taak in het samenwerken met, adviseren aan en ondersteunen van de faculteiten kan vormgeven.

Er wordt niet gerapporteerd over het behalen van doelen richting het CvB, omdat het integraal veiligheidsoverleg geen bestuurlijke entiteit is en derhalve geen eigen tactische of operationele doelen kent. Zij heeft enkel een coördinerende en adviserende functie. Er wordt wel advies uitgebracht (adviesrol) richting het CvB over het eigen functioneren en dat van de centrale staforganisatie (waaronder de SIV) ten aanzien van de verbeteringen of aanvullende ondersteuning die mogelijk nodig zijn.

Operationeel niveau

De faculteiten (in de persoon van de decanen/directeuren) monitoren intern op het behalen van de operationele afspraken en doelstellingen en rapporteren hierover richting het CvB en de centrale staforganisatie.

Hierin zit echter een belangrijk onderscheid:

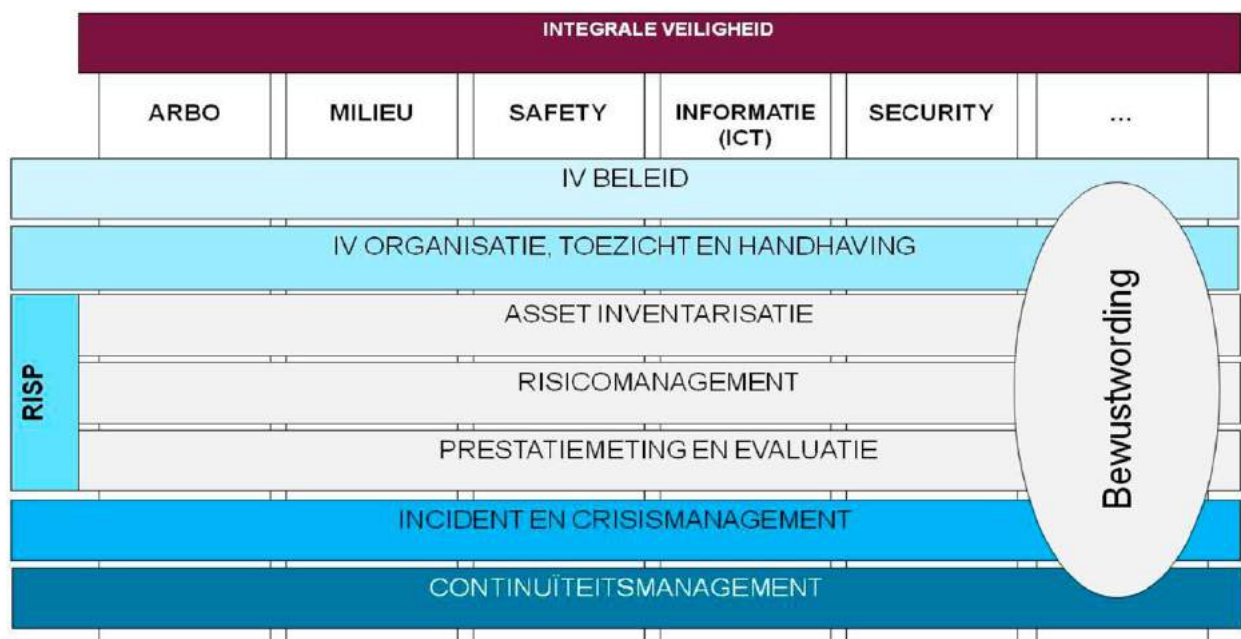
- Richting het CvB wordt enkel gecommuniceerd of de gestelde doelen worden gehaald. Worden de gestelde doelen niet behaald, dan wordt vermeld wat hier de oorzaak van is en wordt een voorstel gedaan voor het nemen van mitigerende maatregelen.
- Richting de centrale staforganisatie wordt gecommuniceerd over het al dan niet behalen van de doelen. Doordat de staforganisatie (en de SIV) hierop monitoren houden zij zicht op de voortgang van de implementatie van het beleid en wordt inzichtelijk op welke onderdelen advies te geven is.

Voordelen van monitoren

- Monitoren, toezicht houden en rapporteren zorgt voor een goede interne controle, inzicht in de organisatie maakt het mogelijk de organisatie tijdig bij te sturen indien gestelde doelen niet behaald worden
- Het juist vormgeven van de rol van monitoren draagt bij aan de noodzaak tot het versterken van de bestuurskracht ten aanzien van het thema IV en continuïteit.

3.4 Bedrijfsvoering van integrale veiligheid

In het eerste deel van dit hoofdstuk is de blauwdruk voor de governance van integrale veiligheid uitgewerkt. In dit deel van hoofdstuk 3 komt de blauwdruk voor de bedrijfsvoering van integrale veiligheid aan bod. Om te komen tot integrale veiligheid (IV) is de inrichting van de volgende generieke veiligheidsprocessen van belang:



Figuur 18. Generieke veiligheidsprocessen

Integraal veiligheidsbeleid

Het IV-beleidsproces is een proces dat zorgt dat er over de functionele kolommen heen één uniforme wijze is voor de totstandkoming van zowel strategisch als operationeel veiligheidsbeleid. Op basis van de vastgestelde risico's dient een beleid geformuleerd te worden hoe met deze risico's om te gaan. In missie, visie en strategische doelstellingen worden keuzes gemaakt met betrekking tot de ambities ten aanzien van veiligheid, voor het accepteren dan wel mitigeren van deze risico's (risicobereidheid). In het beleid worden verantwoordelijkheden voor veiligheid benoemd zoals een wijze van inbedding van veiligheid in de governance structuur, alsook de mate van focus op IV-processen en de uitgangspunten voor de technische, bouwkundige en organisatorische maatregelen. Belangrijke output voor dit proces is een integraal veiligheid beleidsplan. Onderstaande tabel beschrijft de belangrijkste rollen in het beleidsproces:

Beleidsproces	RvT	CvB	Centrale Stafororganisatie	Sectie IV	College Decanen	Staf faculteit
Coördinatie			x	x		
Advisering			x	x		
Uitvoering						x
Besluitvorming		x			x	
Monitoring	x	x	x			

Tabel 3. Rollen in het beleidsproces

Integrale Veiligheidsorganisatie toezicht en handhaving

De veiligheidsorganisatie vormt het hart van integraal veiligheidsbeleid aangezien in dit proces de maatregelen daadwerkelijk worden uitgevoerd. Op basis van het IV-beleid wordt per organisatie-eenheid invulling gegeven aan het beleid. De verantwoordelijkheid voor uitvoering ligt binnen onderdelen van de organisatie (faculteiten) en blijft een lijnbevoegdheid. Daaronder vallen de feitelijke maatregelen, instructies en het integreren van het thema veiligheid in gedragscodes. De vastlegging van deze maatregelen in plannen en procedures vormt een sluitstuk op de set aan maatregelen. Belangrijke output voor dit proces is een organisatiehandboek en operationeel plan. Onderstaande tabel beschrijft de belangrijkste rollen in het Organisatie en handhavingproces:

Organisatie en handhaving	RvT	CvB	Centrale Stafororganisatie	Sectie IV	College Decanen	Staf faculteit
Coördinatie						x
Advisering			x	x		
Uitvoering				x		x
Besluitvorming					x	
Monitoring			x	x		

Tabel 4. Rollen in het organisatie- en handhavingproces

Risico-Inventarisatie en Sturing Proces (RISP)

Op basis van de drie subprocessen: asset inventarisatie, risicomanagement en prestatiemeting en evaluatie wordt binnen integrale veiligheid het risico-inventarisatie en sturing proces vormgegeven:

- Asset inventarisatie

Startpunt van integrale veiligheid is het zicht hebben op de waardevolle “assets” in de organisatie (veiligheidsobjecten). Assets of veiligheidsobjecten zijn de zaken van “waarde” voor de organisatie. Dit kunnen zowel fysieke zaken als immateriële zaken als personen in of imago van de organisatie zijn.

- Risicomanagement

Relevante risicoscenario's worden opgesteld voor de onderkende veiligheidsobjecten en beoordeeld door scores toe te wijzen op impact en voorstelbaarheid. Hiermee wordt een risicoprofiel (het acceptabele risiconiveau) voor de organisatie geschetst welke input is voor het veiligheidsbeleid.

- Prestatiemeting en -bijstelling

Effectiviteit en efficiëntie van de veiligheidsmaatregelen is het uiteindelijke doel. Dan is het ook goed om regelmatig te meten of de huidige set aan maatregelen voldoet. Door het vooraf bepalen van prestatie-indicatoren wordt een raamwerk geboden voor het toetsen van de werking. De resultaten uit metingen vormen input voor het bijstellen van de bestaande opzet en zijn daarmee instrumenten in een continu proces van kwaliteitsverbetering.

Belangrijke output uit dit proces is een risicomatrix, keuze voor accepteren en een dashboard voor monitoring. Onderstaande tabel beschrijft de belangrijkste rollen in het RISP-proces:

RISP	RvT	CvB	Centrale Stafororganisatie	Sectie IV	College Decanen	Staf faculteit
Coördinatie			x	x		
Advisering			x	x		
Uitvoering			x			x
Besluitvorming		x			x	
Monitoring			x		x	

Tabel 5. Rollen in het RISP-proces

Incident en Crisismanagement

Crisismanagement beschrijft het proces dat start zodra er een incident/ crisis voordoet. Na goed risicomanagement is er dus sprake van een incident (ongewenste gebeurtenis) binnen het restrisco welke uitgroeit tot crisis. Hoe wordt gehandeld om zo snel mogelijk het incident/ crisis in een beheersbare vorm terug te dringen. Ook de voorbereiding om te kunnen handelen wordt als onderdeel meegenomen. Belangrijke output van dit proces is een crisisplan en oefenplanning. Onderstaande tabel beschrijft de belangrijkste rollen in het crisismanagement- proces:

Crisis- management	RvT	CvB	Centrale Stafororganisatie	Sectie IV	College Decanen	Staf faculteit
Coördinatie			x	x		
Advisering			x	x		
Uitvoering						x
Besluitvorming		x			x	
Monitoring		x	x		x	

Tabel 6. Rollen in het crisismanagementproces

Continuïteitsmanagement

Continuïteitsmanagement is het proces dat ervoor zorgt dat de organisatie in haar minimale vorm kan blijven door draaien indien er een risico werkelijkheid wordt. Belangrijke output van dit proces is een continuïteitsplan. Onderstaande tabel beschrijft de belangrijkste rollen in het proces van continuïteitsmanagement:

Continuïteits- management	RvT	CvB	Centrale Stafororganisatie	Sectie IV	College Decanen	Staf faculteit
Coördinatie			x	x		
Advisering			x			
Uitvoering						x
Besluitvorming					x	
Monitoring			x	x		

Tabel 7. Rollen in het proces van continuïteitsmanagement

Bewustwording

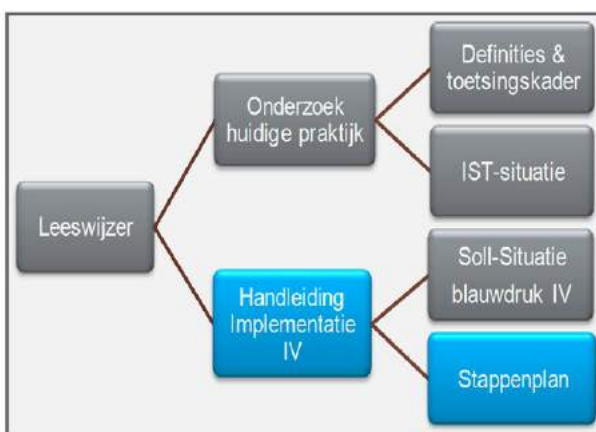
Hoewel bewustwording geen apart proces is, vraagt dit onderwerp specifieke aandacht. Veiligheid effectief binnen organisaties implementeren slaagt alleen indien deze gebaseerd is op een breed draagvlak. Dat betekent dat er niet één persoon of afdeling is die zich met veiligheid bezighoudt maar dat iedereen verantwoordelijk is voor zijn persoonlijke werk/leefomgeving en daar als eigenaar over waakt. Enkel een slot op een deur hebben is niet voldoende, de deur mag dan ook niet open blijven staan. Het gedrag van medewerkers is bepalend of een organisatie daadwerkelijk veilig is. Een bewustwordingstraject is nodig om medewerkers bewust te maken van de veiligheidsrisico's en om deze medewerkers te informeren wat zij zelf kunnen doen. Bewustwording is daarom een element dat in alle processen specifieke aandacht behoeft.

In deze 3e bouwsteen is aandacht besteed aan de Soll-situatie: hoe kan integrale veiligheid het beste binnen de governance en bedrijfsvoering van universiteiten en hogescholen worden ingericht. Nadat de voorgaande bouwstenen de IST-situatie hebben onderzocht, wordt nu naar de toekomstige situatie gekeken aan de hand van een tweetal blauwdrukken. De eerste blauwdruk richtte zich op de governance van IV, een aansturingsmodel op strategisch, tactisch operationeel niveau. De tweede blauwdruk beschrijft vervolgens de processen die in de bedrijfsvoering van de organisaties moeten worden doorgevoerd om Integrale veiligheid te kunnen sturen en te beheersen. Het doel van de twee blauwdrukken is om aan te geven hoe het onderwerp integrale veiligheid binnen het algemene governance model van een instelling kan worden belegd en welke mogelijkheden er zijn om dit onderwerp te sturen en te beheersen.

Stappenplan naar integrale veiligheid

Bouwsteen 4, een stappenplan naar IV

Dit hoofdstuk vormt het sluitstuk op de handleiding IV. Het tekent de route uit naar inbedding van integrale veiligheid in governance en bedrijfsvoering: hoe komt u van IST-situatie naar de Soll-situatie. Deze laatste en meest praktische bouwsteen geeft u de handvatten om alle kennis uit de voorgaande bouwstenen in praktijk te brengen binnen uw eigen organisatie. Het volgen van het implementatiepad brengt u uiteindelijk in de situatie waarin integrale veiligheid binnen uw organisatie is geïmplementeerd en u als manager of bestuurder de veiligheid beheerst waardoor u 'in control' bent.

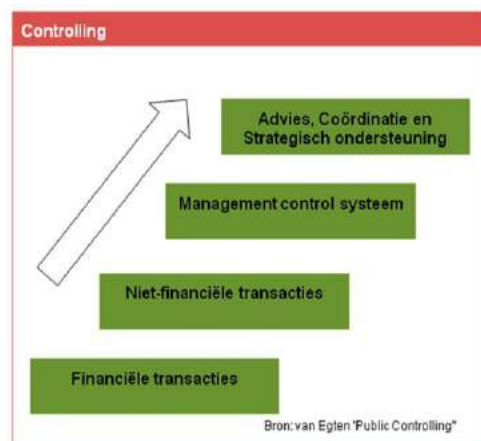


4.1 Inleiding

Om integrale veiligheid goed te organiseren moet de organisatie zowel naar de governance structuur als naar de bedrijfsvoering kijken. In de eerste plaats is de wijze waarop een onderwijsinstelling deze twee pijlers heeft georganiseerd bepalend. Daarnaast bepaalt de ambitie in grote mate welke stappen moeten worden doorlopen. Hierdoor is een generiek stappenplan niet nuttig. In dit hoofdstuk wordt een dynamisch stappenmodel beschreven dat een onderwijsinstelling helpt bij het bepalen van de benodigde activiteiten voor het realiseren van integrale veiligheid. Op basis van vijf groeifasen wordt beschreven wat de vereisten aan governance en bedrijfsvoering zijn voor het realiseren van integrale veiligheid. Een onderwijsinstelling kan daarmee zelf bepalen welke onderdelen zij wel en welke zij niet moet/wil oppakken. Dit stappenplan biedt daarmee een hulpmiddel voor beoordeling van de huidige situatie (toetsingskader), geeft richting aan de te ontwikkelen activiteiten en biedt een houvast voor monitoring van de verbetering op het gebied van integrale veiligheid.

4.2 De ontwikkeling naar integrale veiligheid

Als we kijken naar andere functies in de bedrijfsvoering zien we dat deze functies door de jaren een groei hebben doorgemaakt. De ontwikkeling van integrale veiligheid als volwassen bedrijfs onderdeel heeft overeenkomsten met de groei van de controllers- functie. Prof. Van Egten schetst in haar boek "De controlfunctie in de publieke en non-profitsector"⁹ de groei van van de controlfunctie in een organisatie. In de jaren 50 startte de controlfunctie met



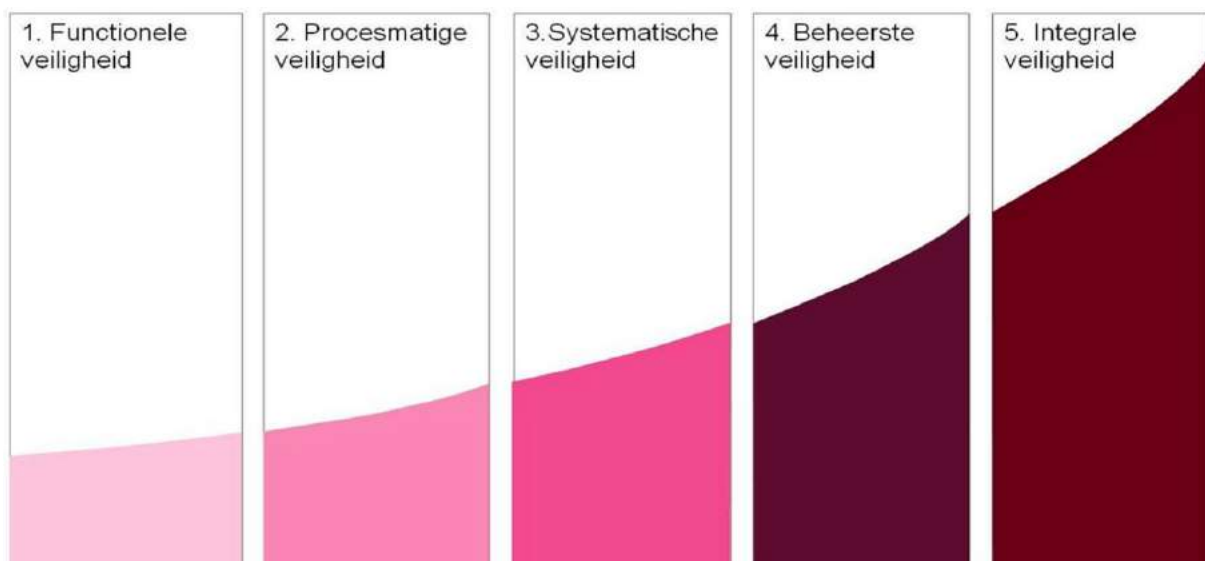
⁹ Public controlling reeks 13, Sdu Uitgevers, 2006

het beheersen van financiële transacties. Later kwamen daar ook niet-financiële transacties bij. Om overzicht te houden ontwikkelt de functie zich nu naar het beheren van een managementcontrolsysteem dat instrumenten bevat zoals risicoanalyses, begrotingen, forecast rapportages, audits en doorlichtingen. Wanneer de controller deze instrumenten bezit is hij in staat om dominante informatiepositie op te bouwen en op basis daarvan strategisch advies te geven aan de top ten behoeve van besluitvorming.

Ook integrale veiligheid zal als bedrijfsfunctie moeten groeien. Voor integrale veiligheid zal een stap gemaakt moeten worden van het functioneel gescheiden monitoren en beheersen van veiligheidsfuncties naar het integraal monitoren en beheersen van alle veiligheidsfuncties. Wij onderscheiden een vijftal verschillende ontwikkelfasen:

1. Functionele Veiligheid
2. Procesmatige veiligheid
3. Systematische veiligheid
4. Beheerste veiligheid
5. Integrale veiligheid

In onderstaand figuur wordt een modelmatige ontwikkeling van veiligheid in de bedrijfsvoering beschreven op basis van deze vijf ontwikkelfasen. Iedere stap bouwt voort op de elementen die belangrijk zijn uit de voorgaande fase.



Figuur 20. Ontwikkelfase voor integrale veiligheid

Functionele veiligheid

Functionele veiligheid is een organisatiegraad in governance en bedrijfsprocessen waarin er sprake is van een vaag of niet gedocumenteerd beleid. De organisatie benadert de verschillende vormen van veiligheid als aparte functionele activiteiten zonder dat er formele processen zijn beschreven. Er is op een afdeling één verantwoordelijke persoon voor arbo veiligheid die op basis van de incidenten in zijn/ haar blikveld acteert. Datzelfde geldt ook voor de andere functioneel verantwoordelijken (ICT, Milieu, etc).

Procesmatige veiligheid

Procesmatige veiligheid is een organisatiegraad waarin per veiligheidsfunctie duidelijk is vastgelegd welk proces wordt uitgevoerd. Voor uitvoering van het proces zijn rollen en verantwoordelijkheden helder vastgelegd. Er wordt binnen een veiligheidsfunctie één taal gesproken in de regelmatige en heldere rapportages over de veiligheidsfunctie.

Systematische veiligheid

Systematische veiligheid is een organisatiegraad waarin per veiligheidsfunctie een organisatiebreed beleid is opgesteld en afgestemd met de verantwoordelijke voor het primaire proces. Bijvoorbeeld: een arbo-coördinator in één organisatie-eenheid benadert arbo-veiligheidszaken op eenzelfde wijze als de arbo-coördinator in een andere organisatie-eenheid. Hiervoor is samenwerking en training binnen de functionele kolom noodzakelijk. Doordat er sprake is van afstemming en samenwerking is het mogelijk om organisatiebreed te rapporteren over de veiligheidssituatie in de functionele kolom.

Beheerste veiligheid

Bij beheerste veiligheid is het lijnmanagement verantwoordelijk voor de veiligheidssituatie. Zij zal geconfronteerd worden met alle functionele veiligheidsfuncties en zal eisen stellen (normen wensen) ten aanzien van de informatie over veiligheid. De verantwoordelijke voor de veiligheidsfunctie zal incidenten moeten kunnen rapporteren, eenduidig beleid moeten formuleren en duidelijke prestatie indicatoren moeten afspreken.

Integrale veiligheid

Integrale veiligheid gaat uit van gelijksoortige processen (bijvoorbeeld risicomanagement, beleidsvorming, crisismanagement, asset inventarisatie) binnen alle veiligheidsfuncties. Dit creëert eenduidigheid en vergelijkbaarheid over de veiligheidsfuncties heen. Er wordt door het lijnmanagement gestuurd op integrale risico's. Het management is in staat om continue verbetering te realiseren op het vlak van veiligheid. Er is sprake van bewustwording ten aanzien van integrale veiligheid bij medewerkers en studenten. Op basis van de veiligheidssituatie is het bestuur in staat om een bestuursverklaring af te geven dat de organisatie "veilig" is (in-control- statement). Bij deze organisatiegraad is de organisatie in staat om zich te vergelijken met collega organisaties (benchmarks) en gebruikt zij integrale veiligheid als competitief voordeel.

4.3 Zes categorieën voor de ontwikkeling naar integrale veiligheid

In paragraaf 1.3 beschreven wij het toetsingskader op basis waarvan de "IST-situatie" van de governance van onderwijsinstellingen is bekeken. Hierin worden vier categorieën beschreven: Strategisch, Tactisch/ operationeel, Toezicht en Verantwoording. In paragraaf 3.3 werd op basis van de vijf verschillende rollen (advies, besluitvorming, coördinatie, uitvoering en monitoring) de governance van integrale veiligheid behandeld, de "SOLL-situatie". In deze paragraaf worden de cruciale processen van integrale veiligheid beschreven. De mate waarin al deze processen binnen de organisatie zijn ingeregeld bepaalt tevens de ontwikkelfase waarin de implementatie van integrale veiligheid op dat moment bevindt. Het stappenplan naar ontwikkeling van integrale veiligheid is zeer divers en afhankelijk van de positie waarin de organisatie zich bevindt en de ambitie die zij zichzelf gesteld heeft. Om het groeipad naar integrale veiligheid inzichtelijk te maken zijn zes categorieën benoemd:

- Categorie 1: Veiligheidsbeleid (strategisch)
- Categorie 2: Organisatie en handhaving (tactisch en operationeel)
- Categorie 3: Risico-inventarisatie en sturingsproces (tactisch en operationeel)
- Categorie 4: Prestatiemeting en evaluatie (verantwoording en toezicht)
- Categorie 5: Crisismanagement en continuïteitsmanagement (tactisch/ operationeel)
- Categorie 6: Bewustwording

Per categorie worden vragen gesteld die passen bij de groeifasen uit het ontwikkelmodel. Door antwoord te geven op deze vragen kan een organisatie per categorie zien hoever de organisatie is in het ontwikkelmodel. Indien een vraag niet beantwoord kan worden, betekent dit een actiepoint voor verdere groei.

Hoe ver deze groei moet gaan hangt af van een aantal vragen:

- Wat is het streefniveau voor de organisatie?
- Welke categorieën vindt de organisatie belangrijk om te ontwikkelen (en welke niet)?
- In welk tijdsinterval moet het gestelde doel bereikt worden?
- Wat is de uitgangssituatie van de organisatie?

4.3.1 Categorie 1: Beleidsproces (strategisch)

Veiligheidsbeleid gaat over het formuleren van een veiligheidsstrategie en bijhorende plannen die in de lijn liggen van de visie en missie van het bedrijf, het daartoe structureren van een veiligheidsorganisatie en het daarbij controleren of de beoogde veiligheidsdoelstellingen wel worden bereikt. Hierbij komt met name de rol naar voren ten aanzien van besluitvorming over veiligheid.

Onderstaande tabel beschrijft de vragen binnen de categorie “Veiligheidsbeleid”, die de organisatie zich moet stellen passend bij de vijf groeifasen naar integrale veiligheid:

Categorie 1: Veiligheidsbeleid (Strategisch)				
1. Functionele Veiligheid	2. Procesmatige veiligheid	3. Systematische veiligheid	4. Beheerste veiligheid	5. Integrale veiligheid
- Is er een veiligheidsbeleid opgesteld? - Hebben functionele afdelingen hun eigen interne veiligheidsbeleid? - Is veiligheid wetgeving gestuurd, voldoet de organisatie aan wet en regelgeving?	- Heeft het management een formele rol bij veiligheid? - Is er een veiligheidsbeleid per veiligheidsfunctie (bijv. safety) binnen de faculteit? - Vindt besluitvorming plaats op niveau van de faculteitsdirecteur?	- Is het lijnmanagement actief betrokken bij veiligheidsbeleid? - Wordt het veiligheidsbeleid per veiligheidsfunctie afgestemd over de faculteiten heen? - Voldoet het veiligheidsbeleid aan externe normen? - Wordt veiligheid organisatiebreed toegepast o.b.v. van risico analyse? - Is er draagvlak voor veiligheidsbeleid? - Wordt een PDCA-cyclus gehanteerd en geborgd? - Zijn (veiligheidsfunctie) overschrijdende processen geïdentificeerd?	- Is er sprake van een missie en visie over veiligheid op strategisch niveau? - Zijn er strategische doelstellingen ten aanzien van veiligheid belegd? - Is er een portefeuillehouder veiligheid binnen het CvB? - Wordt het veiligheidsbeleid periodiek aangepast op basis van ervaringen, risicoanalyse en/of externe normen? - Wordt van toeleveranciers (werkend in de organisatie) geëist dat ze beschikken over een veiligheid management systeem?	- Wordt veiligheid als onderscheidend vermogen (concurrentie voordeel) gebruikt ten opzichte van andere onderwijsinstellingen? - Is het bestuur actief betrokken bij het veiligheidsbeleid? - Draagt het bestuur het beleid uit via openbare stukken (bijv. door middel van afgifte van verklaring van compliance)?

Tabel 8. Groeifasen Veiligheidsbeleid

4.3.2 Categorie 2: Organisatie en handhavingsproces (tactisch en operationeel)

Organisatie en handhaving gaat over het benoemen van rollen, verantwoordelijkheden en instrumenten op tactisch en operationeel niveau. Het richt zich op de wijze van organiseren zodat gestelde strategische doelstellingen gehaald worden.

Onderstaande tabel beschrijft de vragen die organisatie zich moet stellen passend bij de vijf groeifasen naar integrale veiligheid:

Categorie 2: Organisatie en handhaving (tactisch en operationeel)				
1. Functionele Veiligheid	2. Procesmatige veiligheid	3. Systematische veiligheid	4. Beheerste veiligheid	5. Integrale veiligheid
- Is er een (veiligheids)document dat de organisatie en handhaving ten aanzien van veiligheid beschrijft? - Zijn processen en procedures van de veiligheidsfunctie(s) beschreven? - Kenmerkt de veiligheidsaanpak van de organisatie zich als reactief?	- Zijn in het veiligheidsdocument rollen en verantwoordelijkheden vastgelegd? - Zijn in het veiligheidsdocument competentie-eisen beschreven? - Is er een mono-facultair veiligheidsoverleg?	- Vindt coördinatie van veiligheid via een staffunctie plaats? - Is er een systematiek voor het vastleggen van (veiligheid) documenten? - Ligt de primaire uitvoeringsrol van veiligheid bij de afdelingen/ faculteiten? - Is er sprake van een Staf-facultair overleg (samenwerking met ander functionele eenheden in de organisatie op het gebied van veiligheid)? - Is een opleidingsplan onderdeel van het veiligheidsdocument?	- Is het lijnmanagement zich bewust van haar rol ten aanzien van veiligheid en vervult zij deze? - Is het lijnmanagement in staat om proactief risico's te signaleren en maatregelen te initiëren? - Is er een Multi-facultair overleg t.a.v. veiligheid? - Is er strategische besluitvorming door CvB?	- Is er een adviesfunctie voor de stafafdeling IV? - Is er een tactische coördinatiefunctie voor de staf afdeling IV? - Is er een toezichtfunctie voor stafafdeling IV? - Voldoet de organisatie aan externe normering? - Vindt er operationele uitvoering plaats op integrale risico's? - Is er sprake van een inter-facultair veiligheids overleg? - Vindt er tactisch en operationele besluitvorming en coördinatie plaats binnen een inter-facultair veiligheidsoverleg?

Tabel 9. Groeifasen organisatie en handhaving

4.3.3 Categorie 3: Risico-inventarisatie en sturingsproces (tactisch en operationeel)

Een inventarisatie van risico's (in risicomanagement "asset" inventarisatie genoemd) is een noodzakelijke activiteit om beeld te krijgen op de te beschermen onderdelen in de organisatie. Zoals reeds eerder gezegd kan het hier gaan over zowel personen, materiële als immateriële zaken die van essentiële waarde zijn voor de organisatie. Het sturingsproces beschrijft vervolgens hoe op tactisch en operationeel niveau gehandeld dient te worden in relatie tot de geïnventariseerde risico's. Dit sturingsproces noemen we het risicomanagementproces, het is een veel gebruikte term die binnen veel vakgebieden naar voren komt. Een risicomanagementproces bestaat uit de volgende activiteiten:

- risicoscenario identificatie: welke scenario's zijn relevant voor de waardevolle assets van de organisatie?
- risicoanalyse: wat is de kans dat een dergelijk scenario zich voordoet en wat is het gevolg voor de instelling, risico ranking: wat is de score van Kans x impact.

Onderstaande tabel beschrijft de vragen die organisatie zich moet stellen passend bij de vijf groeifasen naar integrale veiligheid:

Categorie 3: Risico-inventarisatie en sturingsproces (tactisch en operationeel)				
1. Functionele Veiligheid	2. Procesmatige veiligheid	3. Systematische veiligheid	4. Beheerste veiligheid	5. Integrale veiligheid
- Is er een overzicht van te beschermen waardevolle objecten en risicovolle processen beschikbaar? - Is er een risico-analyse verricht? Worden zowel fysieke als informatie(kennis) gerelateerde risico's beschouwd?	- Is er een proces beschreven hoe vastgesteld wordt wat de waardevolle objecten en processen zijn in de organisatie? - Is er een risicomanagementproces beschreven en vastgelegd voor de identificatie, analyse en ranking van veiligheid risico's?	- Wordt op een systematische (periodieke, haalbare) wijze (per veiligheidsfunctie) een asset inventarisatie uitgevoerd conform een vastgelegd proces? - Is er een systeem voor uitvoering van risicomanagement?	- Is lijnmanagement en bestuur zich bewust van de te beschermen waardevolle objecten en risicovolle processen binnen de afdeling? - Kent het Lijnmanagement de risico's? - Vindt er periodieke evaluatie plaats van risico's?	- Is er een organisatiebreed overzicht van de waardevolle objecten en waardevolle processen (binnen de verantwoordelijkheid van de organisatie) gezien vanuit alle veiligheidsfuncties (veiligheid, safety, arbo, milieu, informatie)? - Heeft de organisatie een integrale risicomatrix? Matrix met op de ene as de kans, op de andere as de impact. In een integrale risicomatrix worden de risico's vanuit verschillende veiligheidsfuncties (arbo, milieu, safety, veiligheid, informatie) in relatie met elkaar gebracht.

Tabel 10. Groeifasen asset inventarisatie en risicomanagement

4.3.4 Categorie 4: Prestatiemeting en evaluatie (verantwoording en toezicht)

Het goed en beheersbaar organiseren van veiligheid kan niet zonder kritisch meten en evalueren. Dit is de brandstof voor de verbetercyclus. Daar waar er een wettelijke plicht is vormt extern toezicht een stok achter de deur. Alleen een gezonde top-down monitoring en daaraan gekoppeld een verantwoordingsvraag kan zorgen dat ook intern toezicht adequaat wordt geborgd. Intern toezicht geeft zicht op de naleving van strategische doelen en tactisch operationele doelen.

Onderstaande tabel beschrijft de vragen die organisatie zich moet stellen passend bij de vijf groeifasen naar integrale veiligheid:

Categorie 4: Prestatiemeting en evaluatie (verantwoording en toezicht)				
1. Functionele Veiligheid	2. Procesmatige veiligheid	3. Systematische veiligheid	4. Beheerste veiligheid	5. Integrale veiligheid
- Wordt er een "prestatiemeting" ten aanzien van een functioneel veiligheidsgebied uitgevoerd? - Worden er evaluaties gehouden ten aanzien van uitvoering van één of meerdere veiligheidsfuncties (maandcontroles)? - Hoe vaak is er wettelijke toezicht? - Vinden er afdelingsspecifieke incidentenregistratie plaats? - Vinden er afdelingsinterne afhandeling van incidenten plaats?	- Vinden er periodieke rapportage plaats van de implementatie van veiligheid? - Wordt bewaakt dat RI&E's (of andere evaluaties) worden uitgevoerd? - Vindt evaluatie alleen plaats na een incident? - Vindt afdelingsinterne evaluatie plaats? - Is er een evaluatieprotocol (werkwijze) vastgesteld?	- Is er een format voor objectieve en eenduidige rapportage voor het management? - Is er een rapportage van verbeteringen op basis van analyse van incidenten? - Vinden er periodieke audits plaats? - Wordt de inhoud van een evaluatie (RI&E) en opvolging verbeteringen meegenomen in een audit? - Is er controle op verbeteracties? - Is er een afdelingsoverstijgende incidentenregistratie en –afhandeling?	- Is er een organisatiebrede prestatiesturing en evaluatie? - Is er bottom-up verantwoording en topdown monitoring van resultaat gerichte veiligheid? - Zijn er prestatie-indicatoren voor veiligheid vastgesteld? - Wordt het lijnmanagement ook afgerekend op veiligheidsprestaties? - Zijn er afdelingsoverschrijdende audits?	- Zijn de prestatie-indicatoren gekoppeld aan bedrijfsdoelstellingen? - Is er een geïntegreerde audit? - Wordt gebruik gemaakt van benchmarking met andere instellingen op het gebied van veiligheid? - Is er een veiligheidsdashboard beschikbaar?

Tabel 11. Groeifasen prestatiemeting en evaluatie

4.3.5 Categorie 5: Crisismanagement en continuïteitsmanagement (tactisch/ operationeel)

Honderd procent veiligheid is een illusie. Dat betekent dat er altijd incidenten kunnen gebeuren. Soms hebben incidenten zoveel impact dat er een crisis kan ontstaan. Goede voorbereiding door middel van een crisismanagementproces is daarom een vereiste binnen integrale veiligheid. Een calamiteitenplan (ook wel bedrijfs- nood-, of crisisplan genoemd) is een basisvereiste. Hierin wordt vastgelegd hoe men zich voorbereidt op calamiteiten en hoe met calamiteiten om te gaan. Het calamiteitenplan geeft de organisatiestructuren, procedures en afspraken voor calamiteitsituaties. In het plan beschrijft men wie welke taken en bevoegdheden heeft bij calamiteiten en hoe afstemming met andere organisaties plaatsvindt. Continuïteitsmanagement borgt het voortgaan van de meest kritieke processen in de onderwijsinstelling. Het continuïteitsplan stelt de organisatie in staat om kernactiviteiten te continueren of te herstellen. Het plan beschrijft hoe de organisatie zal reageren op een daadwerkelijke verstoring van de meest kritieke processen.

Onderstaande tabel beschrijft de vragen die organisatie zich moet stellen passend bij de vijf groeifasen naar integrale veiligheid:

Categorie 5: Crisismanagement en continuïteitsmanagement (tactisch/ operationeel)				
1. Functionele Veiligheid	2. Procesmatige veiligheid	3. Systematische veiligheid	4. Beheerste veiligheid	5. Integrale veiligheid
- Is er een calamiteitenplan/ noodplan/ crisisplan? - Worden er (operationele) oefeningen georganiseerd als onderdeel van een calamiteitenplan? - Is er een overzicht beschikbaar van kernactiviteiten en processen met prioriteit? - Is er aandacht voor nazorg? Dit is de periode na de bestrijding van een crisis.	- Is er een laagdrempelig meldsysteem voor incidenten? - Zijn calamiteitenprocessen beschreven en vastgelegd? - Worden deze calamiteitenprocessen geoefend? - Zijn alle relevante contactpersonen vastgelegd? - Is er een continuïteitsplan aanwezig dat onderdeel is van het veiligheidsbeleid?	- Worden afdelings-specifieke oefeningen georganiseerd? - Worden organisatiebrede oefeningen georganiseerd? - Worden er bestuurlijke oefeningen georganiseerd? - Is er een continuïteitsplan op basis van een risicoanalyse?	- Is opschaling binnen de organisatie impact gerelateerd? - Vindt er rapportage plaats over incidenten? - Zijn er afspraken met externe organisaties (bevoegd gezag) gemaakt (gemeente, politie, brandweer, GHOR en overige overheden)? - Worden oefeningen met externe partijen georganiseerd (gemeente, politie, brandweer en GHOR)? - Is er een communicatieprotocol tijdens een crisis? - Geeft lijnmanagement uitvoering aansturing aan het continuïteitsplan?	- Heeft de organisatie 1 organisatiebreed crisisresponsplan? - Is er één integraal continuïteitsplan op basis van risicoanalyse, met verschillende scenario's?

Tabel 12. Groeifasen crisismanagement en continuïteitsmanagement

4.3.6 Categorie 6: Bewustwording

Geen veiligheid zonder veiligheidsbewustzijn bij de mensen in de organisatie. Integrale veiligheid kan alleen floreren op een basis van vruchtbare veiligheidscultuur. Een veiligheidscultuur betreft een sociaal verantwoordelijke houding van alle medewerkers ten aanzien van veiligheid in de organisatie.

Onderstaande tabel beschrijft de vragen die organisatie zich moet stellen passend bij de vijf groeifasen naar integrale veiligheid:

Categorie 6: Bewustwording				
1. Functionele Veiligheid	2. Procesmatige veiligheid	3. Systematische veiligheid	4. Beheerste veiligheid	5. Integrale veiligheid
- Zijn de medewerkers voldoende bekend met veiligheidsrisico's en incidenten? - Worden regels door medewerkers voldoende nageleefd? - Wordt veiligheidsgedrag per veiligheidsfunctie geadresseerd?	- Is de veiligheid cultuur beschreven? - Worden bewustwordings-bijeenkomsten georganiseerd voor medewerkers? - Wordt intern gecommuniceerd over veiligheid richting de medewerkers?	- Is veiligheidsbewustzijn een onderdeel van het opleidingsprogramma? - Wordt per veiligheidsfunctie veiligheidsgedrag op een zelfde wijze benaderd?	- Is veiligheid een onderdeel van de beoordelingssystematiek van medewerkers? - Vindt communicatie over veiligheid ook door lijnmanagement plaats (naleving van gemaakte afspraken)? - In hoeverre zijn medewerkers bewust van verschillende van de verschillende gedragsaspecten die voortvloeien uit verschillende veiligheidsfuncties.	- Kunnen medewerkers ook meedenken en -praten over veiligheidsrisico's in een medewerkersplatform? - Om de betrokkenheid bij het veiligheidsbeleid en het draagvlak onder medewerkers voor veiligheidsmaatregelen te vergroten kunnen medewerkersplatforms en overlegstructuren worden ingericht. Medewerkers die dagelijks met beide benen in de praktijk staan kunnen een waardevolle bijdrage leveren aan het bijstellen en doorontwikkelen van maatregelen en beleid.

Tabel 13. Groeifasen bewustwording

Met het bestuderen van deze vierde bouwsteen bent u aan het einde gekomen van de handleiding. Deze laatste bouwsteen biedt een stappenplan om te komen tot de implementatie van integraal veiligheidsbeleid binnen een hoger onderwijsinstelling. Het stappenplan geeft richting aan de te ontwikkelen activiteiten en biedt houvast voor het monitoren van de verbeterinitiatieven op het gebied van integrale veiligheid. De geboden kennis helpt u te bepalen in welke ontwikkelingsfase van integrale veiligheid uw organisatie zich bevindt. Deze bepaling biedt het vertrekpunt voor het maken van een stappenplan voor de verdere ontwikkeling van veiligheidsbeleid voor uw organisatie: het geven van invulling aan de organisatie van integrale veiligheid, het inventariseren van assets en het bepalen en waarderen van risico's, het meten en evalueren van prestaties, het organiseren van crisis- en continuïteitsmanagement en het organiseren van veiligheidsbewustzijn.

Bijlage A Afkortinglijst

BHV	Bedrijfshulpverlening
CvB	College van Bestuur
HBO	Hoger Beroepsonderwijs
HRM	Humane Resource Management
IV	Integrale veiligheid
MT	Managementteam
OCW	Ministerie van Onderwijs, Cultuur en Wetenschappen
OM	Openbaar Ministerie
PDCA	Plan, do, check, act
PIOFAH	Personeel, Informatievoorziening, Organisatie, Financiën, Automatisering/Administratie en Huisvesting
RI&E	Risico-inventarisatie en –evaluatie
RISP	Risico-Inventarisatie en Sturingsproces
RvT	Raad van Toezicht
SIV	Sectie Integrale Veiligheid
SMART	Specifiek, Meetbaar, Acceptabel, Realistisch, Tijdsgebonden
WHW	Wet op het Hoger Onderwijs en Wetenschappelijk Onderzoek
WO	Wetenschappelijk Onderwijs

Bijlage B: Stappenplan integraal veiligheidsrisicomanagement



Toepassing stappenplan

-
- Iedere stap heeft een procesmatige en inhoudelijke component.
 - Per stap vindt u diverse 'tools': nuttige informatie om elke stap inhoudelijk en procesmatig te kunnen verlopen.
 - Het stappenplan kunt u benutten als 'start' van het initiëren van integraal veiligheidsrisicomanagement, maar ook als aanvulling of verdieping op bestaande risicoprofielen.

Toelichting (1/3)

- **Integrale veiligheid.** Veiligheid krijgt in toenemende aandacht binnen het Hoger Onderwijs. Het gaat daarbij om zowel 'traditionele' veiligheidsonderwerpen zoals brandveiligheid, maar in toenemende mate ook over onderwerpen als agressie en geweld en calamiteiten- en crisismanagement. Tegelijkertijd blijft 'veiligheid' een abstract en soms vaag begrip: wat valt er nu wel en niet onder? Ook zijn veiligheidsonderwerpen vaak nog 'gescheiden' onderwerpen, zoals bijvoorbeeld beveiliging aan de ene kant en brandveiligheid aan de andere kant. Er is ook vaak sprake van een functionele scheiding in de organisatie van veiligheid. Als gevolg daarvan worden veiligheidsrisico's ook binnen deze functionele kolommen (afdelingen/ diensten) in kaart gebracht. Ook de partijen buiten de instelling waarmee wordt samengewerkt kunnen per functionele kolom verschillen. Daarnaast kunnen veiligheidsmaatregelen elkaar versterken of kunnen maatregelen gericht op het ene veiligheidsdossier juist contraproductief zijn voor een ander veiligheidsdossier. Nadeel van deze aanpak is dat er voor de bestuurder een gefragmenteerd en soms onbeheersbaar beeld van veiligheid kan zijn. Wanneer u veiligheid daarentegen integraal benadert, probeert u grip te krijgen op alle veiligheidsrisico's in samenhang met elkaar en komt u vervolgens ook tot een passend en samenhangend maatregelenpakket.
- **Veiligheid als één van de belangen.** Er zijn ook andere legitieme belangen, zoals het gewenste onderwijsklimaat, een gezonde bedrijfseconomische situatie, onderzoeks- en onderwijsambities, etc. Het is niet altijd mogelijk om alle belangen tegelijkertijd te dienen. Veiligheid hoeft ook niet altijd het dominante belang te zijn. Een klassiek voorbeeld betreft het mogelijke spanningsveld tussen een gewenste open uitstraling en mogelijk gewenste strengere beveiligingsmaatregelen: mensen vooral binnen laten komen versus het organiseren van controle en obstakels. Veiligheidsrisico's behoeven uiteindelijk altijd een (bestuurlijke) afweging, zeker wanneer andere belangen worden geraakt. Risico's kunnen als gevolg hiervan ook expliciet worden geaccepteerd.

Toelichting (2/3)

- **Doel.** Dit stappenplan is bedoeld om instellingen in het Hoger Onderwijs te faciliteren bij het opstellen van het eigen integrale veiligheidsrisicoprofiel. Met behulp van het stappenplan kan de instelling komen tot maatwerk: dit zijn de risico's die voor mijn eigen organisatie gelden. Door dit periodiek te doen kan het inzicht in risico's en eventuele verschuivingen hierbinnen up to date worden gehouden. Het is geen eenmalige activiteit. Soms verandert de organisatie, veranderen de activiteiten of verandert de omgeving. Dit laatste mogelijk letterlijk wat betreft omliggende gebouwen, bedrijven of infrastructuur of meer figuurlijk in de betekenis van een samenleving die verandert. Door het risicoprofiel aan te laten sluiten op de beleidscyclus krijgt het een vaste plek en levert het ook sturingsinformatie op.
- **Risico's in kaart brengen.** Een risicoberekening ontstaat door de kans te vermenigvuldigen met het effect van een bepaalde onveilige situatie. Het is moeilijk om de risico's (kans en effect) exact te bepalen, maar de waarschijnlijkheid dat iets optreedt, kan wel worden ingeschat. Veiligheidsrisico's zijn deels statisch en deels dynamisch. Bijvoorbeeld door de snel veranderende omgeving en al dan niet getroffen maatregelen kunnen risico's groter of kleiner worden. Ook wijzigingen in de aard of omvang van de studentenpopulatie kunnen van invloed zijn op het risico (bijvoorbeeld meer internationale studenten). Tot slot kan een instelling niet alle veiligheidsrisico's afdichten met maatregelen. Er moet dus een afgewogen keuze plaatsvinden, waarbij proportionaliteit, effectiviteit en efficiency een rol spelen. Er zal daarom ook sprake zijn van een zogenaamd restrisico: het risico dat overblijft (rest) op basis van de maatregelen om de veiligheid te optimaliseren. Het accepteren van het restrisico is een bestuurlijke aangelegenheid.

Toelichting (3/3)

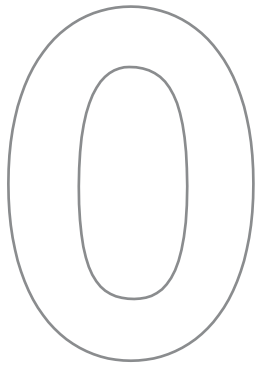
-
- **Proportionaliteit.** Het is geen haalbare kaart om alle veiligheidsrisico's voor een instelling in kaart te brengen. Voor wat betreft de risico's die raken aan de belangrijkste 'assets' van de instelling, is dit echter wel mogelijk en noodzakelijk.
 - **Wat is de relatie tot 'governance'** ('het gehele kader van bedrijfs-, bestuurs- en beheersprocessen dat het mogelijk maakt om het beleid met haar doelstellingen uit te voeren')?
 - Keuzes over het vaststellen van en vervolgens het omgaan met risico's worden mede bepaald door de belangrijkste assets van een organisatie en haar missie, visie en strategische doelstellingen.
 - De rollen en verantwoordelijkheden van sleutelfunctionarissen en de instrumenten die zij tot hun beschikking hebben, zijn van invloed op:
 - het 'eigenaarschap' om met voorstellen te komen om risico's te beperken (mitigeren) en te beheersen
 - het proces dat doorlopen wordt om te komen tot de samenstelling van het risicoprofiel
 - Het risicoprofiel heeft een functie in verantwoording & in toezicht.
 - In termen van 'volwassenheid' geldt dat per volwassenheidsstadium er ook een bepaalde invulling wordt gegeven aan het omgaan met het integrale veiligheidsrisicoprofiel. Dit varieert van:
 - een beperkte scope en meer operationele invulling door enkele sleutelfunctionarissen
 - tot en met een operationeel en bestuurlijk traject waarin op basis van een duidelijke visie op veiligheid, risico-reductie en acceptatie integraal naar risico's wordt gekeken. Het profiel wordt periodiek geactualiseerd

Opbouw stappenplan

0	STAP 0 Initiatieffase: Commitment, opdrachtverwerving & medewerking	• Suggesties om traject in de initiatieffase vorm te geven
1	STAP 1 Opstarten: betrek (interne en externe) partners en verzamel informatie	• Suggesties te betrekken partners • Suggesties te verzamelen informatie
2	STAP 2 Groslijst en selectie: integrale veiligheidsrisico's	• Achtergrondinformatie risico's • Startoverzicht risico's ('groslijst') • Criteria voor selectie • Suggesties voor opzet discussiebijeenkomst • Wat te doen met veiligheidsbeleving?
3	STAP 3 Opstellen en vaststellen risicoparameters: waarschijnlijkheid & impact	• Voorbeelden waarschijnlijkheids- en impactparameters • Ingevuld voorbeeld parameters
4	STAP 4 Wegen risico's & vaststellen risicoprofiel	• Suggesties voor hoe tot weging te komen
5	STAP 5 Interpretatie & prioritering risicoprofiel	• Toelichting bestuurlijke overwegingen bij prioriteringen bepalen maatregelen
6	STAP 6 Borging	• Opstellen actie- en behandelplan: Plan Do Act Check

STAP 0: Initiatieffase

Commitment, opdrachtverwerving & medewerking



zero

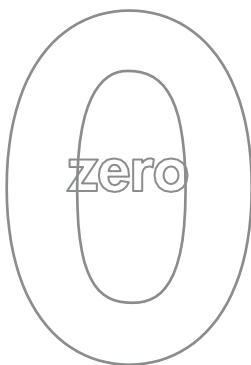
Processtap

- Agendeer het 'integrale veiligheidsstappenplan' bij het College van Bestuur en verkrijg bestuurlijk commitment.
- Verwerf een gelegitimeerde opdracht.
- Maak een projectplan, inclusief planning.
- Breng in kaart wie intern en extern betrokken moeten worden, wat hun behoeften, wensen en belangen zijn en wat hun eventuele rol kan zijn in het project.
- Zorg voor voldoende ondersteuning in mensen, tijd en middelen.

Toelichting:Initiatieffase

Commitment, opdrachtverwerving & medewerking

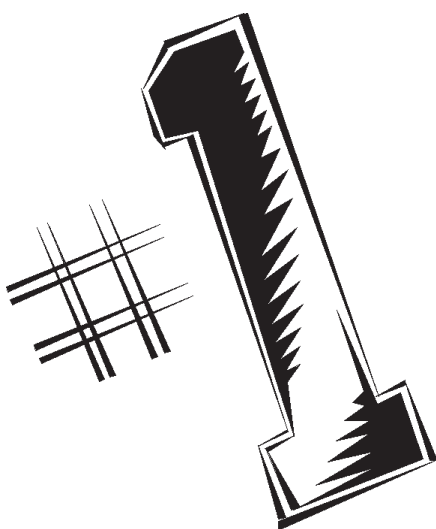
Toelichting stap 0



- Er zijn verschillende manieren om het traject in te gaan om uiteindelijk te komen tot een integraal veiligheidsrisicoprofiel. Wellicht heeft u een opdracht gekregen van het bestuur van de instelling om risico's integraal in kaart te brengen. Bijvoorbeeld vanuit een veiligheidsvisie met als uitgangspunt dat de veiligheidszorg integraal en risicogestuurd vormgegeven wordt binnen de instelling. Misschien bent u juist zelf op het idee gebracht en wilt u ook zelf het initiatief nemen. In dat laatste geval start u door het thema op de bestuurlijke agenda te zetten en het bestuur te verzoeken een verkenning te doen naar de mogelijkheden om te komen tot een integraal veiligheidsrisicoprofiel. Nadat u de verkenning heeft afgesloten, adviseert u het bestuur om het traject te vervolgen met een concrete opdracht. In dit stadium is het belangrijk dat er ook een bestuurlijk trekker is aangewezen en dat er commitment is in de lijndirectie (faculteiten of academies) en de diensten om mee te werken aan een dergelijk traject. Bij verantwoordelijken namens deze organisatieonderdelen is immers ook relevante risico-informatie te halen. Bekijk altijd of er lopende initiatieven of trajecten zijn binnen de organisatie waarbij u logischerwijs kunt aansluiten.
- Stel vervolgens een projectplan op. De doorlooptijd van het project is mede afhankelijk van bestuurlijke ambities, (snelheid in) medewerking die u krijgt van interne en externe partners en de beschikbaarheid en toegankelijkheid van bestaande risico-informatie binnen de instelling.

STAP 1: Opstarten

Betrek (interne en externe) partners en verzamel informatie



Processtap

- Benader interne partners en leg uit wat er verwacht wordt op een aantal momenten binnen het project.
- Verzamel documentatie over veiligheid en risico's (beleid, protocollen, rapportages) in samenwerking met interne en externe stakeholders.

Inhoudelijke stap

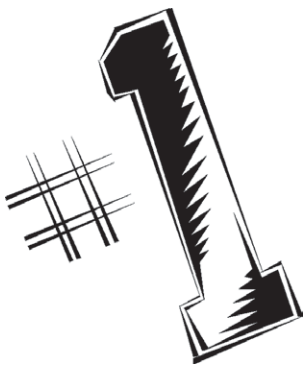
Verzamel:

- 'Neutrale' informatie over locaties en de omgeving (activiteiten gekoppeld aan gebruikers, frequentie/ tijden en ruimtelijke context).
- Incidenten binnen de instelling.

Maak de koppeling tussen informatie en informatiebronnen.

Toelichting: Opstarten

Betrek (interne en externe) partners en verzamel informatie



Hoe interne partners in het project te betrekken en organiseren?

- Er zijn verschillende manieren om interne partners te betrekken in het project. U kunt aansluiten bij een bestaande werkgroep die zich bezighoudt met het thema veiligheid, maar u kunt ook een eigen projectgroep oprichten die op een vast aantal momenten bij elkaar komt (voor stap 1 t/m stap 6). Daarnaast kunt u als projecttrekker op een aantal momenten interne partners binnen de instelling actief betrekken, bijvoorbeeld door interviews af te nemen of een sessie te organiseren.
- In alle gevallen is het belangrijk dat gedurende het project interne partners systematisch betrokken worden en samenwerken:
 - Op elk niveau van de instelling: strategisch & bestuurlijk, tactisch & directie (lijn/ dienst) en operationeel.
 - Namens alle functionele kolommen en met een kijk op zowel sociale als fysieke veiligheid.
- Neem in het projectplan op welke interne partners betrokken worden voor elke stap binnen het stappenplan.

Welke interne & externe partners te betrekken?

Interne partners

- Facilitaire Zaken
- Hoofd beveiliging/ veiligheid
- BHV
- ICT
- Financiën
- Studentenzaken
- Communicatie
- Personeelszaken (HRM)
- Arbo-milieucoördinator
- Secretaris / staf College van Bestuur, etc.
- Onderzoeksafdelingen

Externe partners

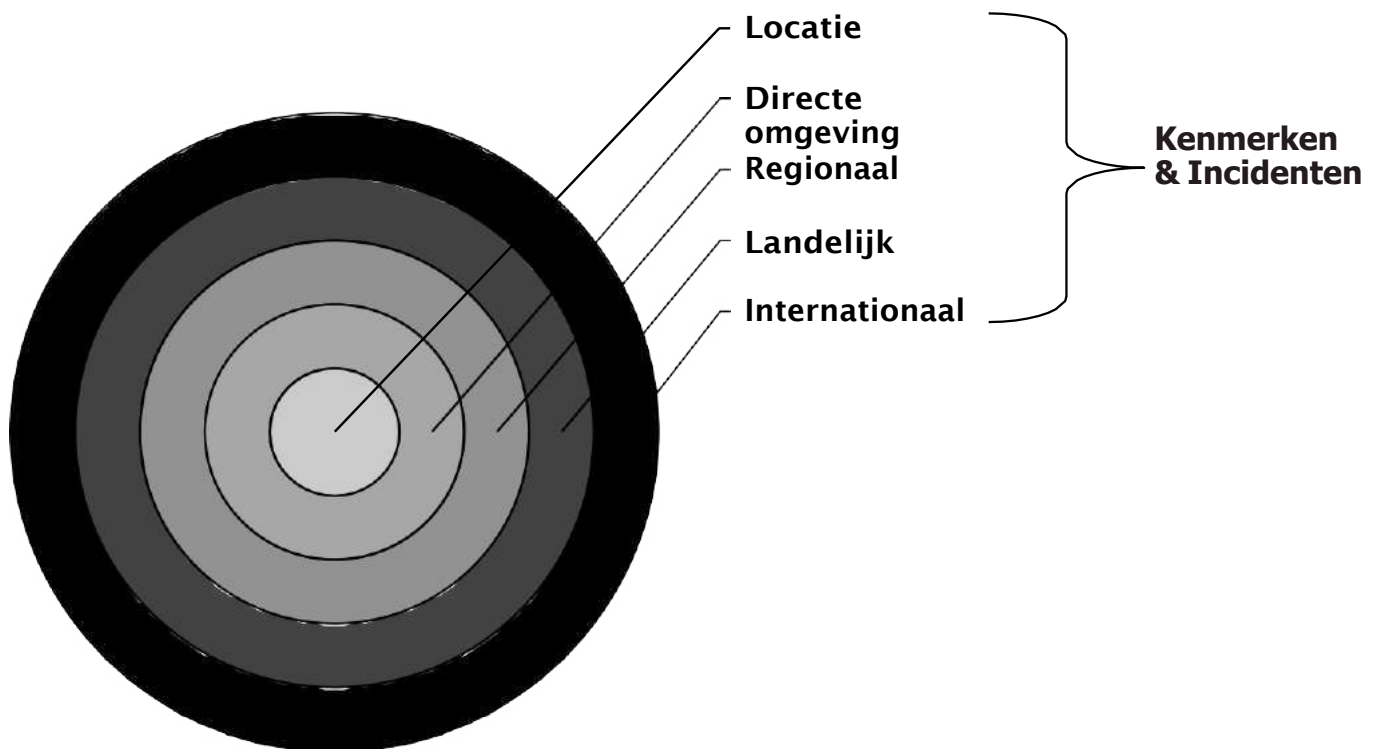
- Brandweer
- Politie
- GGD/GHOR
- Gemeente

Derden die actief zijn op het terrein van de instelling

- Bedrijven
- Onderwijsinstellingen
- Onderzoeksinstituten

Deze externe partijen geven inzicht in mogelijke risico's die zij waarnemen dan wel die samenhangen met de eigen activiteiten van die partijen.

Niveaus van (on)veiligheidsinformatie



Tips

- Bepaal zelf het detail- en schaalniveau van bronnen voor (on)veiligheidsinformatie. Bijvoorbeeld: betrek ik ook dreigingsinformatie (b.v. de kans op aanslag door milieuactivisten) en benut ik meld- en signaleringspunten van gemeente of politie?

Welke (on)veiligheidsinformatie is nuttig om te verzamelen?

- Het actuele visiedocument/ beleidsplan/ jaarplan voor de instelling
- Calamiteiten- en/ of crisisplan
- Informatie over incidenten: jaarrapportages Arbo- en milieumeldingen, registratie beveiligingsincidenten, veiligheidsoverleg, etc.
- Beleidsdocumenten die (mede) gaan over veiligheidsonderwerpen
- Bestaande risico-inventarisaties (o.a. voor wat betreft Arbo: RI&E)
- Bestaande rapportages over veiligheidsbeleving
- Bestaande veiligheidsinstructies of gedragsregels
- Ziekteverzuimcijfers (patronen)
- Overige onderzoeks- en adviesrapporten met betrekking tot veiligheid en risico's of naar aanleiding van calamiteiten

Wat zijn de activiteiten/ diensten en binnen welk organisatieonderdeel vinden ze plaats? 'het DNA van de organisatie'

- Kernactiviteiten: wat zijn de primaire activiteiten van een Hoger Onderwijsinstelling?

Academies/
Faculteiten/ Schools

Onderzoeksafdeling

- Ondersteunende activiteiten, essentieel voor het uitvoeren van de kernactiviteiten. De (staf)diensten zijn hiervoor primair verantwoordelijk, zoals ICT, Financiële en Juridische Zaken, Facilitaire Zaken, Human Resource Management.

(Staf)diensten

- Secundaire activiteiten, alle overige activiteiten, zoals beveiliging, catering, sport, wonen en evenementen, vaak ondergebracht bij diensten of bureaus die daarvoor speciaal in het leven zijn geroepen.

Overige organisatie-
onderdelen en externe organisaties

Wie nemen deel aan die activiteiten, waar vinden ze plaats en hoe vaak? 'het DNA van de organisatie'

Academies/
Faculteiten/ Schools

Bijvoorbeeld: de activiteit **onderwijs**....

- Wie nemen deel aan de activiteiten (**gebruikers**)? Nederlandse en buitenlandse studenten en medewerkers

Waar vinden de activiteiten plaats (**ruimtelijke context**)? Verschillende schaalniveaus: in Nederland of buitenland, stad of platteland, gebouwen, ruimtes etc.

Hoe vaak vinden de activiteiten plaats (**intensiteit en frequentie**)?

Voornamelijk overdag tussen 8:00 en 17:00 uur.

Kies zelf voor het detail- en schaalniveau waarop de vraag beantwoord wordt

Onderwijs

overzicht stap 1

	Activiteiten	Gebruikers	Ruimte en locatie (incl. bewegingen)	Intensiteit en frequentie
De kern- of primaire activiteiten	Onderwijs & wetenschappelijk onderzoek	Studenten in binnen en buitenland, studenten in ontwikkelingslanden (stage)	NL: vier vestigingen in plaats X in de binnenstad, onderdeel Y en Z en buitenland etc.	80% van de onderwijsactiviteiten in NL, 20% buitenland.
De kritieke ondersteunende activiteiten	Laboratorium-werkzaamheden	Medewerkers	Vestiging X en Y	Maandelijks
	ICT	Medewerkers en externen	Vestiging A	24 uur per dag
	Gebouwbeheer	Medewerkers	Alle vestigingen	Renovatie in 2012 gebouw Y
	Beveiliging	Externe inhuur	Alle vestigingen	Gedurende openingstijden
	Energievoorziening	Externe onderhoudsmensen	Ruimte X	Een keer in de maand
Secundaire activiteiten	Wonen	Studenten	Plaats X op het terrein van onderwijsgebouw Y	Een woontoren met 100 bewoners, 24 uur per dag
	Sport	Studenten	Plaats Y aan de rand van de stad	Doordeweekse avonden van 18:00 tot 22:00 uur
	Horeca	Studenten, medewerkers en bezoekers	Elke verdieping van gebouw X	Open van 9:00 tot 17:00 uur
	Evenementen	Studenten, medewerkers en bezoekers	Plaats X, terrein Y	Drie keer per jaar

STAP 2: Groslijst en selectie

Integrale veiligheidsrisico's

2

Processtap

- Bijeenkomst organiseren met interne partners (zie projectplan voor selectie).
- Documentatie uit stap 1 paraat houden.
- Bestuur betrekken bij besluitvorming.

Inhoudelijke stappen

- Breng de maximale set van integrale veiligheidsrisico's in kaart (groslijst).
- Maak vervolgens een risicoselectie voor risico's die gelden voor de specifieke instelling, gegeven haar kenmerken, op basis van locatie, omgevings- en incidenteninformatie en assets.
- Laat de selectie van risico's bestuurlijk vaststellen.

Toelichting: Groslijst en selectie

Integrale veiligheidsrisico's

Hoe een bijeenkomst in te richten om tot selectie te komen?

2

- Het doel is gezamenlijk vaststellen van de veiligheidsrisico's, te komen tot een ruime groslijst met integrale veiligheidsrisico's.
- Bereid u als projecttrekker voor door het verzamelen van informatie (output) uit stap 1.
- Nodig interne partners uit voor een bijeenkomst van minimaal twee uur.
- Vraag deelnemers vooraf na te denken over veiligheidsrisico's die zij waarnemen en/ of in eerder in kaart hebben gebracht.
- Tijdens de bijeenkomst komt u tot een groslijst met veiligheidsrisico's, die u vervolgens nader gaat duiden met elkaar, zodat er uiteindelijk een gezamenlijk beeld ontstaat over wat elk veiligheidsrisico inhoudt.

Welke vragen kan ik de deelnemers stellen om tot selectie te komen?

- Samen met de deelnemers doorloopt u de volgende selectiecriteria voor elk van de integrale veiligheidsrisico's uit de groslijst:
 1. In hoeverre raken ze aan de kernactiviteiten, de kritieke ondersteunende activiteiten en de nevenactiviteiten?
 2. Weten we al iets over de kans en effect uit eerdere risico-inventarisaties, incidentenregistraties, onderzoek (feitelijk en gepercipieerd (veiligheidsbeleving)), historische informatie, et cetera?
 3. In hoeverre raken ze aan de (assets) waarden van de organisatie (imago, mensen, materiële zaken)?
Vaak af te leiden uit de geformuleerde missie, visie en centrale doelstelling van de instelling.

Wat is nuttig om te weten over risico's? (1)

Wat is een risico? 'De mogelijkheid dat een ongewenste gebeurtenis optreedt'

Veiligheidsrisico's vormen een bedreiging voor de instelling. Daarom wil een instelling deze zoveel mogelijk beperken, ter bescherming van o.a.:

- De gezondheid, welzijn en veiligheid(sgevoel) van studenten, medewerkers, en bezoekers
- De waardevolle eigendommen en informatie van de instelling
- De continuïteit van onderwijs en bedrijfsvoering
- Het imago van de instelling

Waar komen veiligheidsrisico's uit voort? O.a. uit het feit dat instellingen in het HO in het algemeen:

- Open(baar) toegankelijk zijn
- Te maken hebben met een zeer diverse studenten- en medewerkerspopulatie en veel interactie tussen mensen plaatsvindt
- Toenemend afhankelijk zijn van ICT voor onderwijs en bedrijfsvoering
- Vaak gebruik maken van externe inhuur en verhuur
- Activiteiten ondernemen met een internationaal karakter, zoals studie en werk in het buitenland
- Op strategisch niveau nog onvoldoende informatie hebben om te sturen op veiligheidsrisico's vanuit een integrale benadering
- Gevolgen kunnen ondervinden van risicovolle activiteiten in de omgeving

Wat is nuttig om te weten over risico's? (2)

Hoe worden veiligheidsrisico's veroorzaakt? Ze kunnen ontstaan door falen of fouten van mensen en/ of het 'systeem' (bijvoorbeeld 'de organisatie', een 'proces'), door natuurlijke oorzaken of door opzet / kwade wil.

Waar in de instelling komen ze voor? Ze kunnen overal in en om de instelling optreden, zowel op fysieke locaties (zoals in een gebouw) als binnen organisatorische onderdelen, zoals een stafafdeling ICT. In eigen land of in het buitenland.

Wat zijn voorbeelden van incidenten die uit veiligheidsrisico's kunnen voortkomen?

- Een grote brand
- Instorting van een gebouw
- Inbraak/ diefstal
- Fraude (financieel of kennis)
- Uitbraak van een infectieziekte
- Een student of medewerker die gewond raakt of overlijdt in het buitenland
- Ernstig geweldsincident

Veiligheidsbeleving meenemen?

Inzicht in de veiligheidsbeleving van medewerkers en leerlingen/ studenten kan belangrijke input zijn voor het verkennen en duiden van risico's.

De beleving dat iets 'een risico' is, betekent niet dat er ook objectief gezien sprake is van een risico. Het kan wel betekenen dat medewerkers of leerlingen worden beïnvloed door eventuele 'zorgen' over risico's, dan wel risico's onderschatten. Indien medewerkers en/of studenten bijvoorbeeld zorgen hebben over de veiligheid 's avonds op het terrein, dan kan dit aanleiding zijn om dit risico als hoger te waarderen.

In veel gevallen gaat de veiligheidsbeleving over sociale veiligheid. Ook fysieke veiligheid kan worden ingebracht in dergelijke onderzoeken. Bijvoorbeeld vragen over de beleving van veiligheid bij proeven, gevaarlijke handelingen, etc.

Indien de veiligheidsbeleving volgens deskundigen niet 'past' bij de 'objectieve' veiligheid, dan kan dit aanleiding zijn om de beleving te willen beïnvloeden. Dit kan bijvoorbeeld door middel van voorlichting.

Welk overzicht van risico's kan ik als 'start' gebruiken (groslijst)?

Sociale veiligheidsrisico's

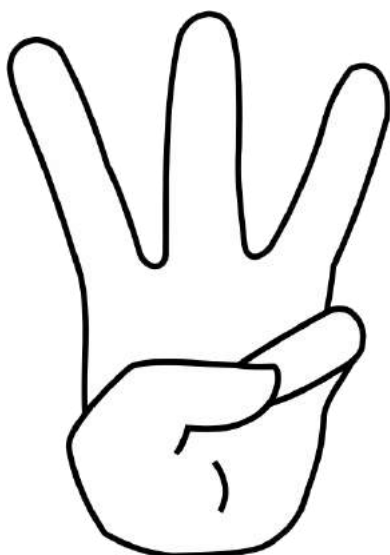
- Verkrijgen of verspreiden van gevoelige digitale informatie
- Fraude (plagiat, tentamenfraude)
- Onbevoegde aanwezigheid
- Agressie & geweld
- Verwervingscriminaliteit
- Discriminatie
- Stalking
- Lekken van informatie
- Seksuele intimidatie of – geweld
- Polarisatie & radicalisering
- Pesterijen
- Middelengebruik
- Vandalisme
- Privacyschending
- Illegale handel
- Gevoel van onveiligheid
- Hacking

Fysieke veiligheidsrisico's

- Brand
- Arbeidsongeval
- Wateroverlast
- Uitval ondersteunende diensten / processen (uitval ICT, elektriciteit, klimaatbeheersing)
- Opslag en gebruik gevaarlijke stoffen
- Ziektegolf
- Verkeersonveiligheid
- Zelfmoord
- Externe veiligheidsrisico's (chemische incidenten, overstroming, extreem weer)
- Explosie
- Instorting
- Hoogrisico locaties omgeving
- Internationaal (algemene categorie voor calamiteiten in het buitenland)

STAP 3: Opstellen en vaststellen

Risicoparameters: waarschijnlijkheid & impact



Processtap

- Bijeenkomst organiseren met interne partners (zie projectplan voor selectie).
- Informatie uit stap 2 betrekken (selectie risico's).
- Bestuur betrekken.

Inhoudelijke stappen

Verzamel:

- Opstellen wegingsparameters.
- (Bestuurlijk) vaststellen wegingsparameters.

Toelichting: Opstellen en vaststellen

Risicoparameters: waarschijnlijkheid & impact



Toelichting

Opstellen parameters

- Het gaat hier om het opstellen van mogelijke categorieën op basis waarvan kans (waarschijnlijkheid) en impact voor de selectie van integrale veiligheidsrisico's (output stap 2) voor de instelling bepaald worden, in samenwerking met interne partners.
- Impactcategorieën zijn bijvoorbeeld 'mensen', 'financiën', 'reputatie' en 'bedrijfsvoering/continuïteit'. Daarom wil een instelling deze zoveel mogelijk beperken, ter bescherming van o.a.:
 - De gezondheid, welzijn en veiligheid(sgevoel) van studenten, medewerkers, en bezoekers
 - De waardevolle eigendommen en informatie van de instelling
 - De continuïteit van onderwijs en bedrijfsvoering
 - Het imago van de instelling'
- Gebruik als uitgangspunt bij de selectie van de impactcategorieën de 'assets' van de instelling: wat is van belang voor de instelling en mag absoluut geen schade oplopen?

Vaststellen parameters

Deze waarschijnlijkheids- en impactcriteria moeten bestuurlijk getoetst, eventueel bijgesteld en vastgesteld worden.

Waarschijnlijkheid				
	1	2	3	4
	Klein Zal bijna nooit voorkomen	Gemiddeld Zal eens in de paar jaar voorkomen	Groot Zal jaarlijks één keer voorkomen	Zeer groot Zal in een jaar regelmatig voorkomen
Impact				
MENSEN Medewerkers, studenten, e.a.	Geen tot nauwelijks lichamelijk of psychisch letsel voor één of meer personen	Geen blijvend lichamelijk of psychisch letsel voor één of meer personen	Blijvend lichamenlijk of psychisch letsel voor één of meer personen	Fataal incident met betrokkenheid van één of meer personen
CONTINUITEIT Organisatie, onderwijs & Kwaliteit	Kortdurende verstoring (enkele uren) van de onderwijsactiviteiten of– kwaliteit op één vestiging of binnen één domein of dienst, zonder merkbare gevolgen voor de continuïteit	Kortdurende verstoring (enkele uren tot een dag) van de onderwijsactiviteiten of– kwaliteit op één vestiging of binnen één domein of dienst, met merkbare gevolgen voor de continuïteit	Merkbare langdurige verstoring (aantal dagen) van de continuïteit van onderwijsactiviteiten of– kwaliteit op één vestiging of binnen één domein of dienst	Langdurige verstoring van de continuïteit van onderwijs- activiteiten of– kwaliteit op meerdere vestigingen tegelijktijd
FINANCIEN Schade & inkomstenderving	< € 5000	€ 5000 – € 250.000	€ 250.000 – € 1.000.000	> € 1.000.000
REPUTATIE Organisatie, opleiding, individue	Nauwelijks negatieve reputatie-effecten	kortstondige negatieve reputatie-effecten	Langdurige negatieve reputatie-effecten (minder dan een jaar)	Meerjarige negatieve reputatie-effecten

STAP 4: Wegen selectie van risico's

4

Processtap

- Bijeenkomst organiseren met interne partners (zie projectplan voor selectie).
- Bestuur betrekken in uiteindelijke weging en vaststelling.

Inhoudelijke stappen

- Verzamel de volgende ingrediënten:
 1. Informatie over (on)veiligheidssituatie (stap 1)
 2. Set van relevante risico's (risicoselectie) (stap 2)
 3. Risicomatrix (waarschijnlijkheid x impact) (stap 3)
 4. Informatie over bestaande maatregelen op de selectie van veiligheidsrisico's.
- Koppel de risico's uit de risicoselectie aan concrete scenario's en kom tot een gedeeld beeld over wat die scenario's inhouden.
- Weeg de scenario's door middel van een stemproces of dialoog. Het resultaat is een concept risicoprofiel.
- Bestuurlijke vaststelling van het risicoprofiel.



Toelichting:

Wegen selectie van risico's

4

Toelichting

- In deze stap worden de veiligheidsrisico's gewogen, zodat er een voorlopig (concept) integrale veiligheidsrisicoprofiel voor de instelling ontstaat. Deze weging is niet wetenschappelijk objectief, maar komt intersubjectief tot stand en benadert daarmee objectiviteit, omdat deze gedragen wordt door meerdere mensen die de organisatie en het proces waarvoor zij verantwoordelijk zijn goed kennen.
- Als voorbereiding moet informatie verzameld worden door interne partners voor wat betreft hun domein en verantwoordelijkheid over getroffen maatregelen op deselectie van integrale veiligheidsrisico's (output stap 2).
- Stel op basis van elk risico uit de selectie van integrale veiligheidsrisico's een scenario op. Bijvoorbeeld: voor het risico 'agressie en geweld': een steekpartij op het terrein van de campus.
- Voor elk scenario wordt de matrix ingevuld en dus beoordeeld op waarschijnlijkheid en impact.
- Maatregelen bepalen uiteindelijk de kans (waarschijnlijkheid) dat een gebeurtenis een bepaalde impact heeft. Deze worden daarom meegenomen in de weging.
- Scenario's met een hoge score op kans en impact behoren tot de toprisico's voor de instelling.
- Het concept risicoprofiel is feitelijk een advies aan het College van Bestuur. Eventueel moet het daarom nadien bij- en vervolgens bestuurlijk vastgesteld worden.

Welke methoden zijn er om tot weging te komen?

- Er zijn diverse methoden om met interne partners tot een weging te komen van elk van de integrale veiligheidsrisico's uit stap 2. Het omzetten van de selectie van risico's naar concrete scenario's maakt het voor betrokkenen makkelijker om na te denken over kans en impact. Wanneer er gewerkt wordt met een matrix, waarin kans en impact uitgedrukt worden in bijvoorbeeld een getal van 1 t/m 4, kan u kiezen voor een kwantitatieve weging door elk van de deelnemers. Het gemiddelde getal voor kans en impact per scenario is dan de uiteindelijke uitkomst voor dat specifieke scenario. Op die manier komt u tot een rangorde per risico/ scenario. De toprisico's, dus de risico's met de hoogst ingeschatte kans en impact komen bovenaan te staan in de ranking.
- U kunt dus kiezen voor een kwantitatieve weging. Daarvoor zijn allerlei softwarepakketten in de markt beschikbaar. U kunt ook kiezen voor een meer kwalitatieve weging, door met de deelnemers van gedachten te wisselen en op die manier tot een ranking te komen.
- In alle gevallen is het belangrijk dat de deelnemers zowel objectieve gegevens over onveiligheid (kwantitatieve 'harde' gegevens, zoals trends in incidenten) als subjectieve gegevens over onveiligheid in ogeschouw nemen (eigen inschatting, metingen van onveiligheidsgevoel).

Hoe kunnen bestaande maatregelen worden 'meegewogen'?

In deze stap vindt een confrontatie plaats tussen de benoemde risico's (scenario's) en de werkelijke maatregelen. Maatregelen kunnen gericht zijn op het verkleinen van de kans dat iets gebeurt en/of op het beperken van de gevolgen als er iets gebeurt.

Een hoger risico kan worden beperkt door middel van adequate maatregelen. Een lager risico waarop geen maatregelen zijn getroffen kan daarmee alsnog als 'zwaarder' worden gezien. Een hoog risico zonder passende maatregelen wordt alleen maar ernstiger. Een laag risico met passende maatregelen wordt kleiner, etc. Inadequate of ontbrekende maatregelen kunnen een reden zijn om een bepaalde activiteit/ een specifiek mogelijk incident als hoger risico te beschouwen.

Soorten maatregelen op hoofdlijnen:

- Inzichtelijke taken, verantwoordelijkheden en bevoegdheden
- Aanwezige expertise & ervaring
- Benodigde capaciteit & middelen
- Compliance aan wet- en regelgeving en interne normen/ regels
- Toezicht & handhaving
- Getroffen maatregelen om incidenten te voorkomen
- Getroffen maatregelen om gevolgen te beperken
- Afspraken met derden

STAP 5: Interpretatie & prioritering risicoprofiel



Processtap

- Agendeer het integrale veiligheidsrisicoprofiel op de bestuurlijke agenda.

Inhoudelijke stappen

- Bestuurlijke interpretatie integraal veiligheidsrisicoprofiel en prioritering aanpak risico's.
- Bestuurlijke vaststelling maatregelen.

Toelichting:

Interpretatie & prioritering risicoprofiel



Toelichting

Interpretatie risicoprofiel

- Het bestuurlijk vastgestelde risicoprofiel geeft inzicht in de toprisico's voor de instelling.
- Het risicoprofiel wordt geïnterpreteerd aan de hand van de risicotolerantie/ risk appetite binnen de instelling: hoeveel risico wil het bestuur van een hoger onderwijsinstelling accepteren, om haar strategische organisatiedoel-einden te bereiken?
- Het integraal veiligheidsrisicoprofiel biedt de mogelijkheid om tot bewuste keuzes over risico-acceptatie te komen.

Prioritering

- Als het gaat om het treffen van maatregelen op deze toprisico's, dan is het realistisch om te bedenken dat daar in elke instelling een kosten-batenanalyse aan vooraf gaat. Afgewogen tegen overige strategische organisatie-doeleinden en belangen. Maatregelen worden getroffen op de belangrijkste onacceptabele (top)risico's. Op de zogenaamde 'restrisico's' worden geen maatregelen getroffen, deze worden als acceptabel bestempeld.
- Het risicoprofiel bevat aangrijpingspunten voor versterking. In een vervolg moet besluitvorming plaatsvinden over eventuele acties en maatregelen op bestuurlijk niveau.

STAP 6: Borging



Processtap

- Organiseer interne partners bij het opstellen van een actie- en behandelplan (zie projectplan voor selectie van partners).

Inhoudelijke stappen

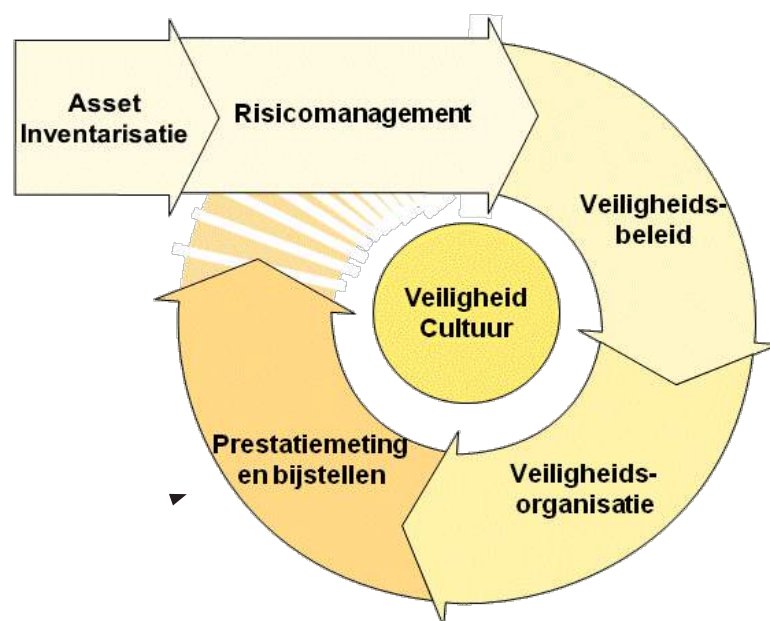
- Het actie- en behandelplan heeft als doel: borging van de bestuurlijk vastgestelde maatregelen.
- Koppeling maatregelen aan planning, mensen en middelen.

Toelichting: Borging

6

Hoe kom ik tot een actie- en behandelplan?

- De acties en maatregelen worden vastgelegd en uitgewerkt in een actie- en behandelplan.
- Idealiter wordt in het actie- en behandelplan een conceptuele koppeling gemaakt tussen de (veiligheids)visie en doelstellingen van de instelling en de maatregelen die daaruit voortvloeien.
Bijvoorbeeld: 'binnen deze instelling wordt veiligheidszorg risicogestuurd ingericht in plaats van incidentgedreven' of 'openbare toegankelijkheid van de instelling is belangrijker dan beveiligingsrisico's'.
- In dit plan is verder opgenomen welke plaats het integrale veiligheids-risicoprofiel krijgt in de Plan Do Act Check cyclus.



Tips voor het implementatieproces, monitoren en evalueren

- In het actie- en behandelplan is opgenomen hoe de maatregelen geborgd worden (voorwaarden voor implementatie), op welke manier gemonitord kan worden of de maatregelen daadwerkelijk uitgevoerd worden en effectief zijn en op welke manier er geëvalueerd kan worden.

Tips voor borging en monitoring:

- Neem de maatregelen mee in prestatieafspraken met verantwoordelijken op alle niveaus van de organisatie (P&O cyclus).
- Laat een bestuurlijk verantwoordelijke of strategisch adviseur (bijvoorbeeld de bestuurssecretaris) periodiek een bestuurlijke rapportage opstellen over de integrale veiligheidsrisico's.

Evalueren risicoprofiel (prestatiemeting en bijstellen):

- Het profiel moet periodiek worden herzien. Wanneer kenmerken wijzigen is een aanpassing mogelijk nodig. Ook trends in daadwerkelijke incidenten dan wel in een specifieke mate van dreiging kunnen aanleiding zijn om het integrale veiligheidsrisicoprofiel aan te passen.
- De 'trekker' heeft een signalerende rol, maar het werkt beter indien verantwoordelijke functionarissen in de organisatie de trekker actief informeren over relevante wijzigingen en ontwikkelingen.
- Een periodieke actieve 'uitvraag' kan helpen: de contactpersonen wordt gevraagd aanpassingen door te geven. Door samen met deze contactpersonen het risicoprofiel ten minste eenmaal per jaar door te spreken wordt ook het risicodenken vastgehouden.
- Het herzien en vaststellen van het integrale veiligheidsrisicoprofiel kan en mag nooit zonder bestuurlijke toestemming tot stand komen.