INTEGRALE
VEILIGHEID
HOGER ONDERWIJS

Management Systeem Integrale Veiligheid

Inhoudsopgave

0 INLEIDING 3

0.1 ALGEMEEN 3

0.2 PROCESBENADERING 4

0.3 BIJDRAGEN 5

1 SCOPE 6

2 NORMATIEVE REFERENTIES 6

3 TERMINOLOGIE EN DEFINITIES 6

VOORBEREIDING 7

4 DE INSTELLING IN ZIJN OMGEVING 7

4.1 DE INSTELLING EN ZIJN OMGEVING 7

4.2 BEHOEFTEN EN VERWACHTINGEN VAN PARTIJEN 7

4.3 REIKWIJDTE VAN HET MIVH 7

4.4 MIVH 7

5 LEIDERSCHAP 8

5.1 LEIDERSCHAP EN BETROKKENHEID 8

5.2 MIVH-BELEID 8

5.3 VERANTWOORDELIJKHEDEN EN BEVOEGDHEDEN 8

PLAN 9

6 PLANVORMING 9

6.1 ACTIES GERICHT OP RISICO'S EN KANSEN 9

6.2 MIVH-DOELEN EN HOE DEZE WORDEN BEREIKT 9

7 ONDERSTEUNING 10

7.1 MIDDELEN 10

7.2 COMPETENTIES 10

7.3 BEWUSTZIJN 10

7.4 COMMUNICATIE 10

7.5 GEDOCUMENTEERDE INFORMATIE 11

7.5.1 Algemeen 11

7.5.2 Maken en bewerken 11

7.5.3 Beheer 11

DO 12

8 WERKING 12

8.1 OPERATIONELE PLANVORMING EN BEHEERSING 12

CHECK 12

9 EVALUATIE VAN DE WERKING 12

9.1 BEWAKING, METING, ANALYSE EN EVALUATIE 12

9.2 INTERNE AUDIT 13

9.3 MANAGEMENT REVIEW 13

ACT 14

10 VERBETERING 14

10.1 NON-CONFORMITEITEN EN CORRIGERENDE ACTIES 14

10.2 VOORTDURENDE VERBETERING 14

Bijlage A Handleiding MIVH

Bijlage B Zelfbeoordeling MIVH

0 Inleiding

0.1 Algemeen

Deze norm is van toepassing op instellingen binnen het wetenschappelijk onderwijs en het hoger beroepsonderwijs.

Dat het 'managen' van integrale veiligheid staat op de agenda's van de Colleges van Bestuur van instellingen voor het hoger onderwijs, volgt direct uit de branchecodes van zowel de VSNU als de Vereniging Hogescholen. Het managen van integrale veiligheid houdt kort gezegd in, dat je welbewuste keuzes maakt in de omgang met risico's (en dat dan ook tot uitvoering brengt). Deze norm gaat daarop in.

Los van branchecodes heeft het management van een instelling simpelweg de plicht om jegens haar stakeholders zorg te dragen voor de continuïteit en het voortbestaan van de instelling. De correcte omgang met risico's brengt dit binnen handbereik.

In dat kader is deze norm een handelingskader ten behoeve van het management, voor planning en besluitvorming die nodig is om voor te bereiden (indien mogelijk: te voorkomen) en te reageren op verstorende incidenten (noodsituatie, crisis of ramp).

Deze norm verhoogt het vermogen van een instelling om een verstorend incident te beheersen en ervan te herstellen en reikt daarvoor alle nodige maatregelen aan om blijvend zorg te kunnen dragen voor de levensvatbaarheid van de instelling.

De kern van deze norm (hoofdstuk 4 en verder) geeft algemene controleerbare criteria voor het vaststellen, controleren, onderhouden en verbeteren van een management systeem ter verbetering van preventie, paraatheid (readiness), mitigatie, respons, continuïteit en herstel van verstorende incidenten.

Invoering van elk managementsysteem vergt de nodige tijd en voldoende managementaandacht en -betrokkenheid. Het is zinloos om in één keer zo'n systeem volledig ingevoerd te willen hebben. De natuurlijke groeiwijze wordt veelal uitgedrukt in volwassenheidsstappen:

1. *Onvoorspelbaar* Problemen worden pas opgelost als ze zich stellen. Processen hebben een chaotisch of ad-hoc karakter.
2. *Herhaalbaar* Beslissingen worden genomen op basis van ervaring. De instelling is zover geprofessionaliseerd (bijvoorbeeld door het invoeren van projectmanagement) dat bij het ontwikkelproces gebruik wordt gemaakt van de kennis die eerder is opgedaan.
3. *Gedefinieerd* De belangrijkste processen zijn gestandaardiseerd.
4. *Beheerst* De kwaliteit van ontwikkelingen wordt gemeten zodat kan worden bijgestuurd.
5. *Geoptimaliseerd* De omgang met risico's verloopt als een geoliede machine en er is alleen maar sprake van fijnafstemming (de puntjes op de i).

Bepaal op welk niveau de instelling zich met betrekking tot integrale veiligheid bevindt en wanneer je op het volgende niveau wilt uitkomen.

0.2 Procesbenadering

Een management systeem bevordert het analyseren van eisen van zowel de instelling als van de belanghebbende anderen en definieert de processen die bijdragen aan het succes van de instelling. Een management systeem biedt een raamwerk voor voortdurende verbetering van veiligheid, paraatheid, respons, continuïteit en incasseringsvermogen. Het biedt de instelling en haar 'klanten' vertrouwen in het vermogen van de instelling om een veilige omgeving te creëren die kan voldoen aan de eisen van de instelling en van de belanghebbenden.

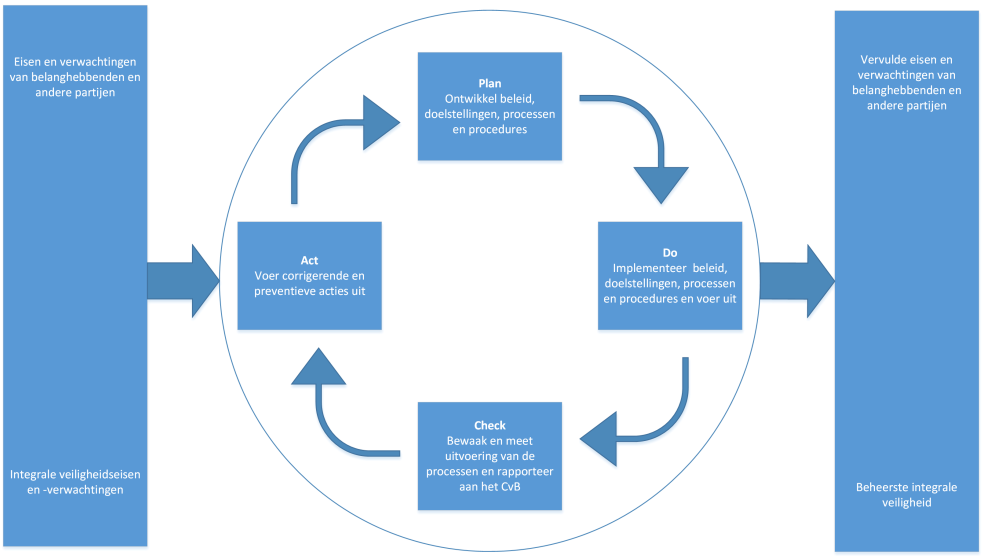
Deze norm hanteert een procesbenadering om (de mate van) integrale veiligheid vast te stellen, te implementeren, uit te voeren, te bewaken, te beoordelen, te onderhouden en voortdurend te verbeteren. Een instelling dient vele activiteiten te identificeren en beheersen teneinde effectief te kunnen functioneren. Elke activiteit die middelen verbruikt en beheerst input omzet in output, kan worden beschouwd als een proces. Vaak zal de output van een proces als input voor een volgende proces worden gebruikt.

De toepassing van een geheel van processen binnen een instelling, samen met de identificatie van de processen en hun management, kan worden beschouwd als een 'procesbenadering'.

De procesbenadering bij een Mivh die in deze norm is beschreven, daagt de gebruikers ervan uit om het belang te benadrukken van:

a. het begrip voor de eisen van de instelling met betrekking tot
   i. risico,
   ii. veiligheid,
   iii. integriteit (visie, normen en waarden, regels en procedures, personeelsbeleid en personeelscultuur, incidenten en handhaven, monitoren en verantwoorden, organiseren en borgen),
   iv. privacy,
   v. veiligheidsketen (pro-actie, preventie, preparatie, repressie en nazorg);
b. het vaststellen van een beleid en doelstellingen om risico's te beheersen;
c. het implementeren van maatregelen om de risico's van de instelling te beheersen binnen de context van de missie van de instelling;
d. het bewaken en beoordelen van de uitvoering en de effectiviteit van het Mivh; en
e. continue verbetering gebaseerd op objectieve metingen.

Deze norm maakt gebruikt van het 'plan-do-check-act' (PDCA) model. Bijgaande figuur illustreert hoe een Mivh de instellingseisen voor integrale veiligheid en de verwachtingen van belanghebbende partijen als input gebruikt en via een reeks processen output levert die voldoen aan de eisen en verwachtingen.



Plan Ontwikkel Mivh-beleid, doelstellingen, processen en procedures die nodig zijn voor integrale veiligheid en om resultaten te kunnen bereiken die in overeenstemming zijn met het algehele beleid en doelstellingen van de instelling.

Do Implementeer het Mivh-beleid, de maatregelen, processen en procedures en voer deze uit.

Check Bewaak en meet de uitvoering van de processen, afgezet tegen het Mivh-beleid, doelstellingen en praktische ervaringen en rapporteer aan de hoogste leiding zodat deze een en ander kan reviewen.

Act Voer corrigerende en preventieve acties uit, gebaseerd op interne audits en management review, om zo voortdurende verbetering te realiseren.

0.3 Bijdragen

Aan de totstandkoming van deze norm hebben velen bijgedragen, waaronder Carla van Cauwenberghe (OWinsp), Beer Franken (AMC), Paul Goossens (Hogeschool Rotterdam), Peter de Groot (Avans), Aldert Jonkman (Vereniging Hogescholen) en Michael Mehrow (Windesheim).

1 Scope

Dit normenkader (kortweg: norm) is gericht op integrale veiligheid binnen instellingen in het hoger onderwijs en de wijze waarop de leiding dat systematisch stuurt (governance). Het biedt daardoor een raamwerk voor het inrichten en uitvoeren van een managementsysteem voor integrale veiligheid in het hoger onderwijs (Mivh).

Mivh biedt tevens aangrijpingspunten voor beoordeling (op basis van self-audits, peer-reviews en externe audits).

De primaire doelgroep van Mivh bestaat uit Colleges van bestuur en Colleges van toezicht.

2 Normatieve referenties

Deze norm sluit aan bij ondermeer:

NEN 7131:2010 Maatschappelijke veiligheid – Managementsystemen voor veiligheid, voorbereiding op incidenten en continuïteit – Eisen en aanbevelingen voor het gebruik

ISO 9001:2008 Quality management systems – Requirements.

ISO 14001:2004 Environmental management systems – Requirements with guidance for use

ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements

ISO 28000:2007 Specification for security management systems for the supply chain

Richtlijn voor de jaarverslaglegging RJ400 (mvo)

Het onderwijscontroleprotocol 2013 (owinsp.nl)

3 Terminologie en definities

In een volgende versie van het Mivh worden terminologie en definities nader uitgewerkt. [1]

[1] Het bepalen van terminologie en definities behoorde niet tot de scope van het deelproject maar dient gelet op eenduidige communicatie in een volgende versie wel toegevoegd te worden.

Voorbereiding

4 De instelling in zijn omgeving

4.1 De instelling en zijn omgeving

De instelling stelt de in- en externe onderwerpen vast die van belang zijn voor het vervullen van zijn doelstellingen (uitgaande van haar missie, visie en verantwoordingsbeleid) en die het beoogde resultaat van het Mivh beïnvloeden.

4.2 Behoeften en verwachtingen van partijen

De instelling stelt vast:

- welke belanghebbenden van belang zijn voor Mivh; en
- welke behoeften de belanghebbenden hebben.

4.3 Reikwijdte van het Mivh

De instelling stelt het bereik en de toepasselijkheid van Mivh vast, teneinde de reikwijdte ervan vast te leggen. Hierbij moeten in overweging worden genomen:

- de in- en externe onderwerpen die in 4.1 werden genoemd; en
- de behoeften die in 4.2 werden genoemd.

4.4 Mivh

De instelling zal een Mivh ontwikkelen, implementeren, onderhouden en continu verbeteren in overeenstemming met deze norm.

5 Leiderschap

5.1 Leiderschap en betrokkenheid

De hoogste leiding van de instelling zal leiderschap en betrokkenheid jegens Mivh tonen door:

- ervoor zorg te dragen dat het Mivh-beleid en de Mivh-doelen worden vastgesteld en in overeenstemming zijn met de strategische koers van de instelling;
- ervoor zorg te dragen dat de Mivh-eisen – die uit de Mivh-doelen voortvloeien – worden geïnternaliseerd in de reguliere processen van de instelling;
- ervoor zorg te dragen dat de middelen die nodig zijn voor Mivh, beschikbaar zijn;
- het belang van een effectieve Mivh en naleving van Mivh-eisen uit te dragen;
- ervoor zorg te dragen dat Mivh diens beoogde resultaten bereikt;
- personen te sturen en te steunen in het bijdragen aan de effectiviteit van Mivh;
- continue verbetering actief uit te dragen; en
- andere niveaus van leiding te steunen in het tonen van leiderschap binnen hun gebieden van verantwoordelijkheid.

5.2 Mivh-beleid

De hoogste leiding van de instelling stelt het Mivh-beleid vast dat:

- passend is voor de doelstelling van de instelling;
- een raamwerk biedt voor het kunnen vaststellen van de Mivh-doelen;
- een zelfverplichting bevat om te voldoen aan de van toepassing zijnde eisen; en
- een zelfverplichting bevat om Mivh voortdurend te verbeteren.

Het Mivh-beleid dient:

- beschikbaar te zijn als officieel vastgesteld document;
- bekend te worden gemaakt binnen de instelling; en
- beschikbaar te zijn voor belanghebbenden, voor zover van toepassing.

5.3 Verantwoordelijkheden en bevoegdheden

De hoogste leiding draagt ervoor zorg dat verantwoordelijkheden en bevoegdheden voor relevante rollen worden toegewezen en bekend wordt gemaakt binnen de instelling.

De hoogste leiding zal verantwoordelijkheden en bevoegdheden toewijzen teneinde:

- ervoor te zorgen dat Mivh zich conformeert aan de eisen van deze norm en
- voortdurend op de hoogte te worden gesteld van de tenuitvoerlegging van Mivh.

Plan

6 Planvorming

6.1 Acties gericht op risico's en kansen

De onderwerpen uit 4.1 en de eisen genoemd in 4.2 zullen bij de planvorming van het Mivh worden betrokken, alsmede de kansen en risico's die zich aandienen bij:

- het zekerstellen dat Mivh zijn doelen kan realiseren;
- het voorkomen of beperken van ongewenste zaken; en
- het bereiken van continue verbetering.

De instelling zal in de planvorming (de planning) betrekken:

- acties die nodig zijn om afdoende met de risico's en kansen om te gaan
- hoe:
    - de acties te integreren en implementeren in de Mivh-processen
    - de effectiviteit van deze acties te evalueren.

6.2 Mivh-doelen en hoe deze worden bereikt

De instelling zal Mivh-doelen vaststellen op relevante niveaus en functies.

De Mivh-doelen dienen:

- consistent te zijn met het Mivh-beleid;
- meetbaar te zijn (indien praktisch uitvoerbaar);
- rekening te houden met van toepassing zijnde eisen;
- te worden bewaakt;
- te worden uitgedragen; en
- bijgewerkt te worden indien nodig.

De instelling zal informatie met betrekking tot de Mivh-doelen documenteren.

Bij het plannen hoe de Mivh-doelen zullen worden bereikt, zal de instelling vaststellen:

- wat dient te gebeuren;
- welke middelen daarvoor nodig zijn;
- wie voor de uitvoering verantwoordelijk is;
- wanneer het volbracht dient te zijn; en
- hoe de resultaten dienen te worden beoordeeld.

7 Ondersteuning

7.1 Middelen

De instelling stelt vast welke middelen nodig zijn om et Mivh te ontwikkelen, implementeren, onderhouden en voortdurende te verbeteren en stelt die middelen beschikbaar.

7.2 Competenties

De instelling dient:

- de vereiste competenties van personeel onder haar gezag vast te stellen die de uitvoering van Mivh (kunnen) beïnvloeden;
- zeker te stellen dat deze personen competent zijn op grond van hun opleiding, training en/of ervaring;
- indien van toepassing actie te ondernemen om de noodzakelijke competenties te verwerven en de effectiviteit van deze actie te evalueren; en
- relevante documentatie te bewaren als bewijs van competentie.

7.3 Bewustzijn

Personen die werkzaamheden onder het gezag of in opdracht van de instelling verrichten moeten bewust zijn van:

- het Mivh-beleid;
- de van hen verwachte bijdrage aan de effectiviteit van Mivh, met inbegrip van de voordelen van een verbeterde Mivh uitvoering;
- de gevolgen van niet-naleving van de Mivh-eisen.

7.4 Communicatie

De instelling dient de noodzaak van in- en externe communicatie die relevant is voor Mivh vast te stellen, met inbegrip van:

- waarover moet worden gecommuniceerd;
- wanneer moet worden gecommuniceerd; en
- aan wie de communicatie moet worden gericht.

7.5 Gedocumenteerde informatie

7.5.1 Algemeen

Het Mivh van de instelling omvat tenminste:

- gedocumenteerde informatie die krachtens deze norm verplicht is;
- gedocumenteerde informatie die de instelling heeft aangegeven als noodzakelijk voor de effectiviteit van het Mivh.

7.5.2 Maken en bewerken

Bij het maken of bewerken van gedocumenteerde informatie zal, indien van toepassing, de instelling zorgdragen voor:

- identificatie en beschrijving (bijvoorbeeld titel, datum, auteur of referentienummer);
- formaat (bijvoorbeeld taal, software versie, figuren) en media (bijvoorbeeld op papier of elektronisch); en
- beoordeling en goedkeuring qua geschiktheid en toereikendheid.

7.5.3 Beheer

Gedocumenteerde informatie die is vereist door het Mivh of deze norm moet worden beheerst zodat:

- het beschikbaar en geschikt is voor gebruik, op de plaats en tijd waar het nodig is; en
- het afdoende is beveiligd (bijvoorbeeld tegen schending van vertrouwelijkheid, onjuist gebruik of verlies van integriteit).

Voor het beheer van gedocumenteerde informatie zal, voor zover van toepassing, de instelling de volgende activiteiten onderscheiden:

- verspreiding, toegang, opvraging en gebruik;
- opslag en behoud, met inbegrip van behoud van leesbaarheid;
- beheer van wijzigingen (bijvoorbeeld versiebeheer); en
- bewaartermijn en vernietiging.

Do

8 Werking

8.1 Operationele planvorming en beheersing

De instelling moet de processen plannen, implementeren en beheersen die nodig zijn om de eisen te vervullen en de acties die bepaald zijn in 6.1 te implementeren, door:

- criteria voor de processen vast te stellen;
- het beheer van de processen in overeenstemming met de criteria te implementeren; en
- gedocumenteerde informatie bij te houden voor zover nodig om vertrouwen te hebben dat de processen zijn uitgevoerd zoals gepland.

De instelling zal geplande wijzigingen beheersen en de gevolgen beoordelen van ongeplande wijzigingen, daarbij acties uitvoerend om negatieve gevolgen te mitigeren indien noodzakelijk.

De instelling zal ervoor zorgdragen dat uitbesteedde processen worden beheerst.

Check

9 Evaluatie van de werking

9.1 Bewaking, meting, analyse en evaluatie

De instelling bepaalt:

- wat moet worden bewaakt en gemeten;
- de methodes voor bewaken, meten, analyseren en evalueren om geldige resultaten te bereiken;
- wanneer moet worden bewaakt en gemeten;
- wanneer de resultaten van bewaking en meting moeten worden geanalyseerd en beoordeeld.

De instelling zal relevante gedocumenteerde informatie bewaren als bewijs van de resultaten.

De instelling zal de uitvoering van Mivh beoordelen alsmede de effectiviteit ervan.

9.2 Interne audit

De instelling zal met geplande tussenpozen interne audits uitvoeren om informatie te verkrijgen of het Mivh:

a. conformeert aan
   - de eisen die de instelling heeft gesteld aan het Mivh en
   - de eisen die volgen uit deze norm;
b. effectief is geïmplementeerd en onderhouden.

De instelling zal:

a. één of meer auditprogramma's plannen, vaststellen, implementeren en onderhouden, met inbegrip van methoden, verantwoordelijkheden, planningseisen en rapportage. Een auditprogramma zal het belang van de betreffende processen en de uitkomsten van voorafgaande audits hierin betrekken;
b. de auditcriteria en het bereik van elke audit bepalen;
c. auditors selecteren en de objectiviteit en onpartijdigheid van het auditproces bewaken;
d. bewerkstelligen dat de auditresultaten worden gerapporteerd aan het relevante management; en
e. de gedocumenteerde informatie bewaren als bewijs van het audit-programma en de auditresultaten.

9.3 Management review

De hoogste leiding zal met geplande tussenpozen het Mivh beoordelen, teneinde de voortdurende geschiktheid, toereikendheid en effectiviteit vast te stellen.
In de management review worden de volgende overwegingen betrokken:

a. de status van acties naar aanleiding van vorige management reviews;
b. wijzigingen in ex- en interne aangelegenheden van belang voor Mivh;
c. informatie over de uitvoering van Mivh, waaronder ontwikkelingen omtrent:
d. non-conformiteiten en correctieve acties,
e. bewakings- en metingsresultaten en
f. auditresultaten; en
g. mogelijkheden voor continue verbeteringen.

De uitkomsten van een management review zullen ondermeer beslissingen ten aanzien van continue verbetering en de noodzaak voor eventuele wijzigingen van Mivh omvatten.

De instelling bewaart gedocumenteerde informatie als bewijs voor de uitkomsten van management reviews.

Act

10 Verbetering

10.1 Non-conformiteiten en corrigerende acties

Wanneer zich een non-conformiteit zich voordoet, zal de instelling:

a. reageren op de non-conformiteit en
   - actie ondernemen om het te beheersen en corrigeren en
   - de gevolgen afhandelen;

b. de noodzaak van acties beoordelen voor het elimineren van de oorzaken van de non-conformiteit, zodat deze niet wederom optreedt of zich elders voordoet, door:
   - de non-conformiteit te beoordelen;
   - de oorzaken van de non-conformiteit vast te stellen en
   - vast te stellen of zich vergelijkbare non-conformiteiten voordoen of mogelijk kunnen optreden;

c. de nodige acties implementeren;

d. de effectiviteit van elke corrigerende activiteit beoordelen; en

e. indien nodig wijzigingen in Mivh aanbrengen.

Corrigerende acties zijn in overeenstemming met de non-conformiteit die is ontstaan.

De instelling bewaart gedocumenteerde informatie als bewijs van:

- de aard van de non-conformiteiten en de acties die naar aanleiding daarvan zijn genomen,
- de resultaten van de corrigerende acties.

10.2 Voortdurende verbetering

De instelling zal de geschiktheid, toereikendheid en effectiviteit van Mivh voortdurend verbeteren.

Bijlage A

Handleiding MIVH

INTEGRALE
VEILIGHEID
HOGER ONDERWIJS

Inhoudsopgave

Voorwoord 3

Leeswijzer 6

0 Inleiding 7

0.1 Managementsysteem Integrale Veiligheid Hoger Onderwijs (MIVH) 8

0.2 Waarom een managementsysteem voor integrale veiligheid? 8

0.3 Relatie met het instellingsbeleid 9

0.4 Synergie op integrale veiligheid 11

0.5 Volwassenheidaanpak 12

1 Scope 13

2 Normatieve referenties 13

3 Terminologie en definities 14

4 De instelling en zijn omgeving 15

4.1 Instelling en zijn omgeving 15

4.2 Behoeften en verwachtingen van partijen 16

4.3 Reikwijdte van het MIVH 17

5 Leiderschap 17

5.1 Leiderschap en betrokkenheid 17

5.2 MIVH-beleid 19

5.3 Verantwoordelijkheden en bevoegdheden 19

6 Planvorming 20

6.1 Acties gericht op risico's en kansen 20

6.2 MIVH-doelen en hoe deze worden bereikt 23

7 Ondersteuning 25

7.1 Middelen 25

7.2 Competenties 26

7.3 Bewustzijn 26

7.4 Communicatie 27

7.5 Gedocumenteerde informatie 27

8 Werking 28
8.1 Operationele planvorming en beheersing - algemeen 28
8.2 Arbeidsomstandigheden 28
8.3 Milieuveiligheid 29
8.4 Sociale veiligheid 29
8.5 Integriteit 30
8.6 Informatieveiligheid 31
8.7 Privacy 31
8.8 Kennisveiligheid 32
8.9 Internationalisering 33
8.10 Gebouwveiligheid 34
8.11 Crisismanagement, BHV, BCM 35
9 Evaluatie van de werking 36
9.1 Bewaking, meting, analyse en evaluatie 37
9.2 Interne audits 38
9.3 Management review 38
9.4 Evaluatie per veiligheidsthema 39
10 Verbetering 42
10.1 Non-conformiteiten en corrigerende acties 42
10.2 Voortdurende verbetering 43

Bijlage 1: Bronnen 44
Bijlage 2: Raamwerk voor planning van doelen en acties van het MIVH 52
Bijlage 3: Relaties tussen dreigingen, te beschermen belangen en veiligheidsthema's 58
Colofon 62

Voorwoord

Over deze handleiding
Het project ‘Integraal Veilig Hoger Onderwijs’ ondersteunt instellingen in het hoger onderwijs bij het integraal omgaan met veiligheidsvraagstukken. Dit doet zij door expertise te bundelen, samen op te trekken en handreikingen te bieden om risico’s te monitoren, beheersbaar te maken en te houden.

In het deelproject ‘Governance’ is een ‘Managementsysteem Integrale Veiligheid Hoger Onderwijs’ (MIVH) gedefinieerd als hulpmiddel om sturing te geven op integrale veiligheid. Dit document is een handleiding voor het MIVH. Deze handleiding is bedoeld als hulp bij het verder vormgeven van veiligheid in instellingen. Het geeft verwijzingen naar bruikbare aanpakken op de verschillende veiligheidsthema’s. In het verlengde hiervan is een vragenlijst opgesteld die bruikbaar is voor een zelfbeoordeling.

Deze handleiding is de eerste in zijn soort voor het hoger onderwijs. Hiermee bieden we handvatten om vanuit een integrale benadering synergie te bereiken op het veiligheidsbeleid. Wat direct opvalt, is hoe breed het veiligheidsterrein van een instelling is. De handleiding kan als kapstok worden gezien met verwijzingen naar praktische aanpakken op deelterreinen. En op elementen waarop synergie kan worden gehaald met een integrale aanpak. Deze handleiding moet beschouwd worden als een startdocument dat gaande weg verder vorm krijgt.

Kernelementen van een managementaanpak op veiligheid
Een managementbenadering op veiligheid bestaat uit een aantal aspecten die in samenhang functioneren.

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

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

Regels en procedures

De waarden en normen worden geconcretiseerd en ondersteund door het geheel van formele regels en procedures in de organisatie. Ze vinden hun weerslag in de Interne Administratieve Organisatie en Interne Controle. Thema's die daarin van belang zijn, zijn onder andere:

- de opzet van interne toezicht- en auditsystemen,
- beschrijvingen van werkprocessen en risico beheersende maatregelen zoals het vier-ogen-principe,
- functiescheiding en –roulatie,
- het bestuur- en beheersreglement,
- vigerende wet- en regelgeving (ABW, WHW en overig), branche- en gedragscodes
- en studentenstatuut.

Het is essentieel om regelmatig na te gaan of bestaande regels en procedures werken en doen wat ze moeten doen. Effectiviteit hangt immers samen met integraliteit.

Personeelsbeleid en cultuur

Een belangrijk onderdeel van het personeelsbeleid is aandacht voor integraliteit, waaronder aandacht voor integriteit. Het begint al bij de werving en selectie van personeel. Is screening noodzakelijk en zo ja, hoe ver ga je? Ook in diverse personeelsgesprekken (jaarplan, voortgangs- en beoordelings- en exitgesprek) is integriteit een onderwerp dat niet mag ontbreken. Daarnaast zijn ambtseed-sessies, introductiebijeenkomsten, werkoverleggen en integriteitstrainingen aangewezen momenten om te werken aan het verbeteren van de cultuur van de organisatie en het bewustzijn van de medewerkers. Bewustzijn van de veiligheidsrisico's in het hoger onderwijs is een zaak voor alle bestuurders, medewerkers en studenten.

Monitoring en verantwoording

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

Incidenten en handhaving

Waarden, normen en regels zijn alleen zinvol als iedereen zich eraan houdt. Het aanpakken van schendingen geeft het signaal af dat er aan naleving en voorbeeldgedrag (integer handelen) waarde wordt gehecht. Het bekrachtigt de bestaande normen en verkleint het risico op toekomstige schendingen. Het opzetten van handhavingsbeleid is een essentieel onderdeel van het integraal veiligheidsbeleid. Daarin horen onder andere, thuis: regels rondom het onderzoek, het sanctioneren en communiceren van (vermoedens van) misstanden/detecteren en beheersbaar maken van risico's. Voorzieningen gericht op het omgaan met incidenten zoals meldingenregelingen, vertrouwenspersonen en onderzoeksprotocollen maken onderdeel uit van het integraal risicomanagement binnen hogescholen en universiteiten met betrekking tot veiligheidsvraagstukken.

Organiseren en borgen

De aandacht voor veiligheidsvraagstukken in het hoger onderwijs, waaronder integriteit en informatie- en kennisveiligheid, wordt duurzaam en samenhangend binnen de organisatie georganiseerd en geborgd. Bestuurders zijn integraal verantwoordelijk voor het resultaat van hun instelling. Dit betekent niet alleen dat ze onderwijs en onderzoek van kwaliteit moeten leveren, maar ook dat financiële en ondersteunende

systemen op orde moeten zijn. Het hoger onderwijs maakt deel uit van het publieke domein en heeft een maatschappelijke opdracht. Daarbij horen openheid, transparantie en als bestuurder ‘in control’ zijn op alle terreinen. Oog hebben voor integrale veiligheid en integer bestuurlijk handelen is essentieel.

Verdere ontwikkeling van deze handleiding
Wij benadrukken dat deze handleiding de eerste in zijn soort is voor het hoger onderwijs. Uit deze handleiding blijkt dat er op bepaalde veiligheidsterreinen veel bruikbare aanpakken zijn, maar dat op andere terreinen nog weinig beschikbaar is. Wij stimuleren lezers en gebruikers van deze handleiding om mee te denken op praktische aanpakken. Dit kan door het aangeven van verwijzingen naar een praktische aanpak van een instelling die ook bruikbaar kan zijn voor andere instellingen. Wij kunnen ons ook voorstellen dat op bepaalde vraagstukken van de managementaanpak gezamenlijke initiatieven zullen worden ontplooid om daarop verder inhoud en vorm te geven. Een volgende versie van deze handleiding zal op deze bijdragen worden verrijkt.

De deelprojectgroep Governance.

Leeswijzer

Er zijn drie documenten die opvolgend zijn ontwikkeld en samenhangen in het gebruik:

1. Het Managementsysteem Integrale Veiligheid Hoger Onderwijs (MIVH). Dit MIVH is voorzien van toetsbare elementen.
2. Deze handleiding op het MIVH. De handleiding geeft methodes en instrumenten die toegepast kunnen worden op het MIVH en gaat in op de verschillende veiligheidsthema's van een instelling. In deze handleiding zijn verwijzingen opgenomen naar diverse bruikbare methodes en instrumenten.
3. Zelfbeoordelingsinstrument. Dit betreft een vragenlijst die bruikbaar is als zelfbeoordeling op het MIVH.

De handleiding heeft dezelfde hoofdstukindeling als het MIVH. Het is zinvol om eerst het MIVH te lezen en daarna de handleiding. Het MIVH bestaat uit een aantal inleidende hoofdstukken. Daarna worden de onderwerpen behandeld in de zogenoemde plan-do-check-act cyclus.

Daarnaast geeft de handleiding een overzicht op veiligheidsonderwerpen die kunnen spelen bij een instelling. Deze veiligheidsthema's komen vooral ter sprake in hoofdstuk 8 (werking), hoofdstuk 9 (evaluatie van de werking) en in de bijlagen (bronnen en relaties tussen dreigingen, te beschermen belangen en veiligheidsthema's).

0 Inleiding

Hogescholen en universiteiten hebben een complexe maatschappelijke opdracht. Zo voeren instellingen voor hoger onderwijs wettelijke taken uit op het gebied van onderwijs, onderzoek en kennisvalorisatie. Ze hebben een aanzienlijke mate van autonomie bij de uitvoering van die taken. Die uitvoering vindt veelal plaats in grote en complexe organisaties, waarbinnen voortdurend – soms lastige – belangenafwegingen moeten worden gemaakt.

Om de kwaliteit van de uitkomsten en de zorgvuldigheid van de procedures te waarborgen zijn checks & balances nodig. De Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW) voorziet daarin. Het instellingsbestuur – het college van bestuur – is op grond van de WHW integraal verantwoordelijk voor het bestuur en beheer van de instelling. Dat betekent dat het college van bestuur *verantwoordelijk is voor* en *verantwoording aflegt* over de kwaliteit van onderwijs en onderzoek, het naleven van wet- en regelgeving en de omgang met de geldende branchecode, waaraan hogescholen en universiteiten zich hebben gecommitteerd.

In hun afzonderlijke Code voor Goed Bestuur hebben de Vereniging Hogescholen, VH[1], en de Vereniging van Universiteiten, VSNU,[2] met hun leden gezamenlijke afspraken hebben gemaakt over 'goed bestuur', kort gezegd over adequaat beheer en beleid en effectief intern toezicht in het hoger onderwijs. De memorie van toelichting bij de Wet Versterking besturing geeft aan dat een branchecode voor goed bestuur het vertrouwen van de maatschappelijke omgeving in het functioneren van instellingen versterkt. Het speelt een belangrijke rol bij de horizontale verantwoording. Een code biedt ook flexibiliteit en ruimte om anders dan via wettelijke regels vast te leggen hoe instellingen binnen een branche hun verantwoordelijkheid voor goed bestuur waar maken.

Soms gaat er iets mis of doet zich een probleem voor, waardoor instellingen risico's lopen en de veiligheid in het geding is. Onderwijsinstellingen kunnen in de problemen komen als er, bewust of onbewust, onverantwoorde risico's worden genomen. Die risico's worden soms onvoldoende onderkend vanwege gebrekkige deskundigheid of doordat de risico's niet inzichtelijk zijn gemaakt. Van onderwijsinstellingen mag worden verwacht dat ze op sectorniveau inzichten met elkaar delen, normen ontwikkelen en elkaar aanspreken op hun gedrag. De ontwikkeling en toepassing van governance codes speelt een belangrijke rol in het versterken van het zelfcorrigerend vermogen van de sectoren.[3]

In het kader van het project 'Integraal Veilig Hoger Onderwijs' heeft de sector hoger onderwijs, in samenspraak met brancheverenigingen, ministerie en instellingen voor hoger onderwijs de handen ineen geslagen om instrumenten en handreikingen te ontwikkelen die instellingen kunnen ondersteunen bij het integraal hanteren van veiligheidsrisico's. Tools en processen zijn beschikbaar, nu gaat het erom te laten zien dat (en hoe) ze werken, binnen de instellingen afzonderlijk en in de sector hoger onderwijs als geheel.

---

[1] De Vereniging Hogescholen hanteert het naleven van de branchecode als lidmaatschapseis voor de vereniging; zie: http://www.verenigingenhogescholen.nl/bedrijfsvoering/goed-bestuur

[2] Zie: http://www.vsnu.nl/code-goed-bestuur.html

[3] Zie: http://www.rijksoverheid.nl/ministeries/ocw/documenten-en-publicaties/kamerstukken/2013/04/20/kamerbrief-versterking-bestuurskracht-onderwijs.html

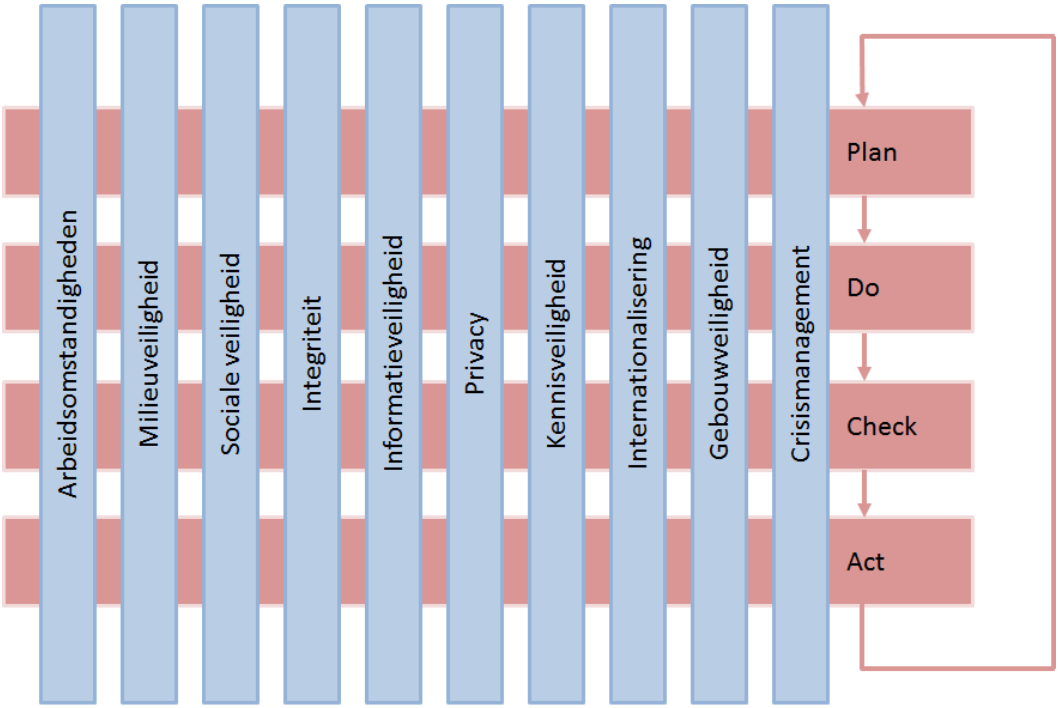
0.1 Managementsysteem Integrale Veiligheid Hoger Onderwijs (MIVH)

Vanuit de Projectgroep Integrale Veiligheid is een Managementsysteem Integrale Veiligheid Hoger Onderwijs (MIVH) ontwikkeld als hulpmiddel om op veiligheid te sturen. Instellingen hebben op deelgebieden al veel gedaan. Het overzicht op veiligheidsonderwerpen inclusief de benadering hiervan ontbreekt veelal. Het MIVH is hiervoor bedoeld.

Dit document is een handleiding op het MIVH. Deze handleiding geeft tips en bevat verwijzingen naar externe normen, handreikingen en overlegorganen voor de specifieke veiligheidsthema's. De hoofdstukindeling van deze handleiding volgt de indeling van het MIVH.

0.2 Waarom een managementsysteem voor integrale veiligheid?

Uit diverse ontwikkelingen van veiligheidsthema's blijkt dat de benodigde activiteiten het beste vanuit een managementsysteem benadering worden uitgevoerd. Hiermee stimuleer je dat relevante verbanden worden gelegd tussen de activiteiten, dat doelstellingen centraal staan, dat er verantwoording mogelijk is naar belanghebbenden en dat verbetering wordt nagestreefd. Een gebruikelijke benadering van een managementsysteem is een indeling van activiteiten in een PDCA (plan-do-check-act) cyclus. Veiligheidsthema´s worden vaak gefragmenteerd benaderd. In eerste instantie staan vaak de incidenten en de maatregelen centraal, in een later stadium richt de aanpak zich meer op visie, risicobeheersing en managementaanpak van het veiligheidsthema. Het resultaat kan zijn dat binnen een instelling diverse managementsystemen op verschillende veiligheidsthema's naast elkaar bestaan, maar dat het overzicht ontbreekt. Zo wordt er mogelijk te weinig op samenhang en synergie gestuurd.



Managementsysteem Integrale Veiligheid Hoger Onderwijs

Het MIVH is direct afgeleid van de High Level Structure voor managementsystemen en volgt de PDCA-cyclus die binnen alle managementsystemen van ISO aanwezig is. Verschillende managementsysteem normen, maar ook eigen instellingsnormen kunnen hier eenvoudig op worden 'ingeplugd'. Vanuit management optiek is er logischerwijs behoefte aan één management systeem om integraal alle veiligheidsaspecten van een organisatie te beheren.
Veiligheidsthema's overlappen elkaar en grijpen op elkaar in. Het veiligheidsthema 'Internationalisering' gaat gepaard met diverse veiligheidsvraagstukken en heeft bijvoorbeeld overlap met de thema's 'Sociale veiligheid', 'Kennisveiligheid' en 'Informatieveiligheid', maar is ingestoken vanuit internationale uitwisseling van studenten, medewerkers en kennis. Het beleid op al deze thema's moet afgewogen en consistent zijn. Het MIVH is een hulpmiddel om te sturen op deze consistentie.

0.3 Relatie met het instellingsbeleid

Met de wet Versterking besturing is de WHW in 2010 gewijzigd op een aantal belangrijke onderdelen. Het gaat met name om de voorwaarden voor goed bestuur en een goede rechtspositie van studenten, het bevorderen van de onderwijskwaliteit en de internationale positie van het hoger onderwijs. Deze wijzigingen zijn met name doorgevoerd om de universiteiten en hogescholen beter in staat te stellen om de opdracht te vervullen die de Nederlandse kennissamenleving hen oplegt, aldus de Memorie van Toelichting[4]. De Vereniging Hogescholen (VH) en de Vereniging van Universiteiten (VSNU), hebben voor hun leden in de afzonderlijke Codes voor Goed Bestuur de afspraken over 'goed bestuur' vastgelegd.

[4] Kamerstukken II 2008-2009, 31 821 nr. 3, blz. 1

De Vereniging van Universiteiten heeft in 2013 de ‘Code goed bestuur universiteiten 2013’ herzien. Hierin is het volgende opgenomen ten aanzien van de risicobeheersing:

> 2.1.5 Het college van bestuur legt de interne risicobeheersings- en controlesystemen voor aan de raad van toezicht.

Figuur 1 Artikel uit Code goed bestuur universiteiten

De Vereniging Hogescholen heeft in 2013 de ‘Branchecode goed bestuur hogescholen’ aangepast en vastgesteld. Nieuw in de Code goed bestuur is de verplichting voor het CvB om in het jaarverslag inzicht te geven in de werking en de belangrijkste resultaten van het interne risicomanagementsysteem. Met de vaststelling van de code verplichten de hogescholen zich jaarlijks de naleving te monitoren en over de uitkomsten ervan te spreken in het verband van de Vereniging Hogescholen. Deze branchecode gaat onder meer in op het hebben van een risicomanagement systeem en een rapportage via het jaarverslag. Het voornemen is dat de monitoring van de veiligheidsrisico’s geschiedt mede aan de hand van het instrumentarium van Integrale Veiligheid Hoger Onderwijs . Het MIVH is bedoeld als één van de risicobeheersings- en controlesystemen voor universiteiten en hogescholen. Het geeft de bestuurder handvatten om op de veiligheidsrisicobeheersing te sturen en daarover verantwoording af te leggen.

II.1.2 Het college van bestuur is verantwoordelijk voor de naleving van de relevante wet- en regelgeving en voor het beheersen van de risico's verbonden aan de uitoefening van de primaire taken van de hogeschool, te weten onderwijs, onderzoek en kennisvalorisatie, alsmede aan de overige instellingsactiviteiten.

II.1.3 Het college van bestuur draagt zorg voor de aanwezigheid en werking van een op de hogeschool toegesneden intern risicomanagement systeem. Als instrumenten van zo'n systeem hanteert de hogeschool in ieder geval:

a) een beschrijving van de belangrijkste risico's die zijn verbonden aan de uitoefening van de primaire taken en de overige instellingsactiviteiten en van de daarop toegesneden beheersmaatregelen;
b) een integriteitcode die in ieder geval op de website van de hogeschool wordt geplaatst;
c) handleidingen voor de inrichting van de financiële verslaggeving, de bekostigingsgegevens en het kwaliteitsbeleid ten aanzien van onderwijs en onderzoek alsmede de voor de opstelling daarvan te volgen procedures;
d) een continuïteitsparagraaf die aan de hand van financiële kengetallen inzicht geeft in de ontwikkeling van de financiële positie van de hogeschool;
e) een systeem van monitoring en rapportering.

II.1.4 In het jaarverslag geeft het college van bestuur inzicht in de werking en de belangrijkste resultaten van het interne risicomanagementsysteem.

II.1.5 Het college van bestuur draagt er zorg voor dat werknemers zonder gevaar voor hun rechtspositie de mogelijkheid hebben te rapporteren over vermeende onregelmatigheden van algemene, operationele en financiële aard binnen de hogeschool aan de voorzitter van het college van bestuur of aan een door hem aangewezen functionaris. Vermeende onregelmatigheden die het functioneren van leden van het college van bestuur betreffen worden gerapporteerd aan de voorzitter van de raad van toezicht. De klokkenluiderregeling wordt in ieder geval op de website van de hogeschool geplaatst.

II.1.6 Het college van bestuur draagt er zorg voor dat studenten en medewerkers zonder gevaar voor hun eigen studieloopbaan of rechtspositie de mogelijkheid hebben te rapporteren over ongewenst gedrag aan een door het college van bestuur aan te wijzen functionaris. De regeling ongewenst gedrag wordt in ieder geval op de website van de hogeschool geplaatst.

Figuur 2 Samenvatting van de Branchecode goed bestuur hogescholen

0.4 Synergie op integrale veiligheid

Het MIVH draagt bij aan de integrale benadering van veiligheidsthema's, waarbij in eerste instantie thema's onderbelicht kunnen blijken. Deze handleiding maakt veel verwijzingen naar normen, handreikingen, good practices, informatiebronnen en overlegorganen. Deze kunnen gebruikt worden om het MIVH voor de instelling specifiek te maken. Dan worden ook de dwarsverbanden tussen de veiligheidsthema's duidelijk, inclusief aspectgebieden die nog niet goed geregeld zijn.
Zodra het MIVH inhoud krijgt op en vanuit de verschillende veiligheidsthema's wordt duidelijk waar synergie mogelijk is. Het sturen op veiligheidsbewustzijn (awareness) en kennisontwikkeling bij een specifieke doelgroep zal bijvoorbeeld integraal voor meerdere veiligheidsthema's kunnen plaatsvinden, in plaats van dat deze doelgroep vanuit verschillende bewustwordingsprogramma's wordt benaderd. Dit is

slechts één voorbeeld; die synergie wordt ook bereikt bij bijvoorbeeld risicoanalyse, maatregelenselectie, organisatie, uitvoering, documentatie, evaluatie en verantwoording.

0.5 Volwassenheidaanpak

Een managementaanpak kan op verschillende niveaus van integratie worden uitgevoerd. Bij de invoering en verbetering van het MIVH is het nuttig om het volwassenheid concept te gebruiken. Deze aanpak is behulpzaam bij het gefaseerd invoeren van het MIVH, waarbij nadruk wordt gelegd op die activiteiten die bij die fase van volwassenheid het meeste nut geven.

Een voorbeeld van een volwassenheidsschaal is de volgende:

Initial	Onvoorspelbaar (chaotisch) en ad hoc. Problemen worden pas opgelost als ze zich stellen.
Repeatable	Het niveau waarbij de organisatie zover geprofessionaliseerd is (bijvoorbeeld door het invoeren van projectmanagement) dat bij het ontwikkelproces gebruik wordt gemaakt van de kennis die eerder is opgedaan. Beslissingen worden dus genomen op basis van ervaring.
Defined	Het niveau waarbij de belangrijkste processen zijn gestandaardiseerd (en dus ook zijn vastgelegd).
Managed	Het niveau waarbij de kwaliteit van het ontwikkelproces wordt gemeten zodat het kan worden bijgestuurd.
Optimized	Het niveau waarbij het ontwikkelproces als een geoliede machine loopt en er alleen maar sprake is van fijn afstemming (de puntjes op de i).

De aanpak kan worden gebruikt om na te gaan wat het huidige niveau is van volwassenheid op integrale veiligheid en op de verschillende veiligheidsthema's. Waar zitten onevenredigheden met heel lage volwassenheid ten opzichte van het gemiddelde? Het verbeteren van die aspectgebieden heeft dan het meeste nut. Ook kan de aanpak helpen om als bestuur de doelstellingen voor het MIVH te bepalen. Welk volwassenheidsniveau wordt nagestreefd ('stip op de horizon') en wat zijn de doelstellingen van het MIVH voor het komende jaar of twee jaar?

Bij een volwassenheidsaanpak hoort ook een auditmodel en daarvoor zijn al twee bruikbare hulpmiddelen voorhanden:

- SURF heeft een normenkader en benchmark model gebaseerd op ISO27002 voor informatiebeveiliging, continuïteit van bedrijfsgegevens en privacy, Hierbij is het helder op welk niveau van volwassenheid de informatiebeveiliging van de instelling zich bevindt.
- ASIS International heeft een handleiding en normenkader met zes volwassenheidsniveaus ontwikkeld voor de NEN 7131 Organizational Resilience Management System (ANSI/ASIS SPC.4-2012, Maturity Model for the Phased Implementation of the Organizational Resilience Management System).

1 Scope

Veiligheid is een breed begrip en doorsnijdt praktisch alle activiteiten van een instelling. Bij het praktisch maken loopt men al snel tegen de definitievraag aan van typen veiligheid die de instelling onderscheidt. Dat moet in het MIVH van een instelling helder worden omschreven. In het MIVH is het veiligheidsdomein van een instelling opgedeeld in de volgende veiligheidsthema's: Arbeidsomstandigheden, Milieuveiligheid, Sociale veiligheid, Integriteit, Informatieveiligheid, Privacy, Kennisveiligheid, Internationalisering, Gebouwveiligheid en Crisismanagement.

Daarnaast is het praktisch om het MIVH stapsgewijs te ontwikkelen en in te voeren. In relatief korte tijd kan het MIVH worden ingevoerd en daarmee ervaring opgedaan. In een volgende 'ronde' kan het MIVH dan worden uitgebreid met een bredere scope. Hierbij zijn verschillende aanpakken mogelijk. Gestart zou kunnen worden om het MIVH in te voeren op alle veiligheidsdomeinen op één locatie. Met de ervaringen op die locatie kan in de volgende ronde het MIVH uitgerold worden over de hele instelling. Een andere aanpak is om het MIVH eerst te implementeren voor enkele vertrouwde veiligheidsdomeinen in de hele instelling en in een volgende ronde het MIVH uit te breiden met de overige veiligheidsdomeinen.

Deze handleiding is bedoeld voor managers en medewerkers van Instellingen voor Hoger Onderwijs die zijn belast met het implementeren, beheren en verbeteren van verschillende veiligheidsthema's. Nadrukkelijk is het de bedoeling dat die activiteiten voor deze veiligheidsthema's integraal en cyclisch worden benaderd.

Bovendien kan deze handleiding ondersteunen bij self-audits en peer-reviews met vragenlijsten.

2 Normatieve referenties

De volgende normatieve referenties ondersteunen het gebruik van dit MIVH:

- ISO Guide 83 'High level structure and identical text for management system standards and common core management system terms and definitions'. Dit een beschrijving van het kernmanagementsysteem waarop alle ISO managementsysteemnormen zijn afgestemd. Bij een actualisering van een ISO managementsysteem zal de structuur van de nieuwe managementnorm worden aangepast conform deze ISO Guide 83.
- NEN-EN-ISO 19011 - Richtlijnen voor het uitvoeren van audits van managementsystemen. Deze richtlijnen kunnen worden gebruikt voor het opstellen en uitvoeren van onderzoeken, reviews en audits van het MIVH.
- NEN-ISO 31000 Risicomanagement – Principes en richtlijnen. Dit is een raamwerk en een procesbeschrijving voor het managen van risico's en is met name bedoeld om integraal verschillende type risico's van een organisatie te managen (enterprise risk management). Deze principes en richtlijnen kunnen voor het managen van risico's binnen het MIVH worden toegepast.

Vanuit veiligheidsdomeinen sluiten de volgende managementsystemen aan op het MIVH:

- NEN 7131 Maatschappelijke veiligheid – Managementsystemen voor veiligheid, voorbereiding op incidenten en continuïteit – Eisen en aanbevelingen voor het gebruik. Dit is een management systeem op 'organizational resilience' en richt zich op security, incidentenbehandeling en continuïteitmanagement.

- ISO 14001 Environmental management systems – Requirements with guidance for use. Dit is het managementsysteem voor milieuveiligheid.
- OHSAS 18001, Occupational Health and Safety Assesment Series. Dit is het managementsysteem voor arboveiligheid.
- NEN-ISO 22301:2012-06, Maatschappelijke veiligheid – Managementsystemen voor bedrijfscontinuïteit – Eisen. Dit is het managementsysteem voor bedrijfscontinuïteit.
- ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements. Dit is het managementsysteem voor informatiebeveiliging.

3 Terminologie en definities

Voor eenduidige communicatie met belanghebbenden binnen en buiten de instelling is het van belang om heldere definities te hebben van begrippen. Deze begrippen zijn meestal gedefinieerd in de documenten van de verschillende veiligheidsthema's. Voor integrale sturing kan het nuttig zijn om centraal een definitielijst aan te leggen en te communiceren. [5]

Voorbereiding

Een geïmplementeerd MIVH is uiteindelijk een continu management proces met mechanismen om de aanpak van veiligheidsvraagstukken doorlopend te verbeteren. Maar hoe komt deze cyclus op gang? Dit onderdeel van het MIVH gaat in op de voorbereiding op de invoering van een MIVH en bestaat uit de hoofdstukken 'De Instelling en zijn omgeving' en 'Leiderschap'.

De invoering van het MIVH kan het beste als een project worden voorbereid en aangestuurd. Houdt daarbij in de gaten dat het MIVH een sociaal-organisatorisch systeem is dat actief door het management wordt ondersteund. Dit gebeurt alleen als het MIVH nauw gerelateerd is aan de organisatie- en bestuursdoelstellingen. Voorts moeten in korte tijd resultaten bereikt worden. Ieder managementsysteem stuurt op resultaten. Bij het kiezen van de scope van het MIVH en het opstellen van het projectplan moet het duidelijk worden dat binnen enkele maanden concrete resultaten bereikt zullen zijn. Dit zowel in de verbetering van de veiligheidssituatie als in de methodiek van het MIVH. Vaak is het zinvol om het MIVH eerst in één organisatieonderdeel of bij één proces in te voeren. Op basis van de successen en de leerervaringen kan daarna het MIVH breder worden ingevoerd. Ook zal het MIVH zoveel mogelijk ingevoerd moeten worden door personen die er daarna ook mee gaan werken. Dit betekent dat teamleden getraind moeten worden in de aanpak en werkwijze van het MIVH, waarna zij dit vertalen naar de risicobeheersing van de eigen processen en veiligheidsdomeinen. Invoering is daarmee direct ook bewustwording en draagvlak creatie bij de belanghebbenden van het MIVH. Een MIVH is per definitie planmatig. Een effectief MIVH heeft eisen en doelstellingen waaraan het moet voldoen, is consistent en richt zich op het continu verbeteren van de veiligheid en van het management systeem.

[5] Het bepalen van terminologie en definities behoorde niet tot de scope van het deelproject maar dient gelet op eenduidige communicatie in een volgende versie wel toegevoegd te worden.

4 De instelling en zijn omgeving

4.1 Instelling en zijn omgeving

Inzicht in de eigen organisatie en omgeving is essentieel om de reikwijdte van het MIVH te kunnen afbakenen, het projectplan en business case op te stellen. Op basis van die inzichten en documenten kan het bestuur een besluit nemen op implementatie van een MIVH.

Voordat gestart wordt met het actief opbouwen van inzicht in de instelling en zijn omgeving, wordt de voorlopige reikwijdte van het MIVH vastgelegd. Welke onderdelen van de instelling vallen wel of juist niet binnen het bereik van het MIVH? Een onderdeel dat niet in scope zit, hoeft dan niet in kaart te worden gebracht. Overigens kan in het vooronderzoek blijken dat de eerste gedachte op scope-bepaling niet effectief is. In de stap 4.3 (reikwijdte van het MIVH) wordt de uiteindelijke scope van het MIVH vastgelegd.

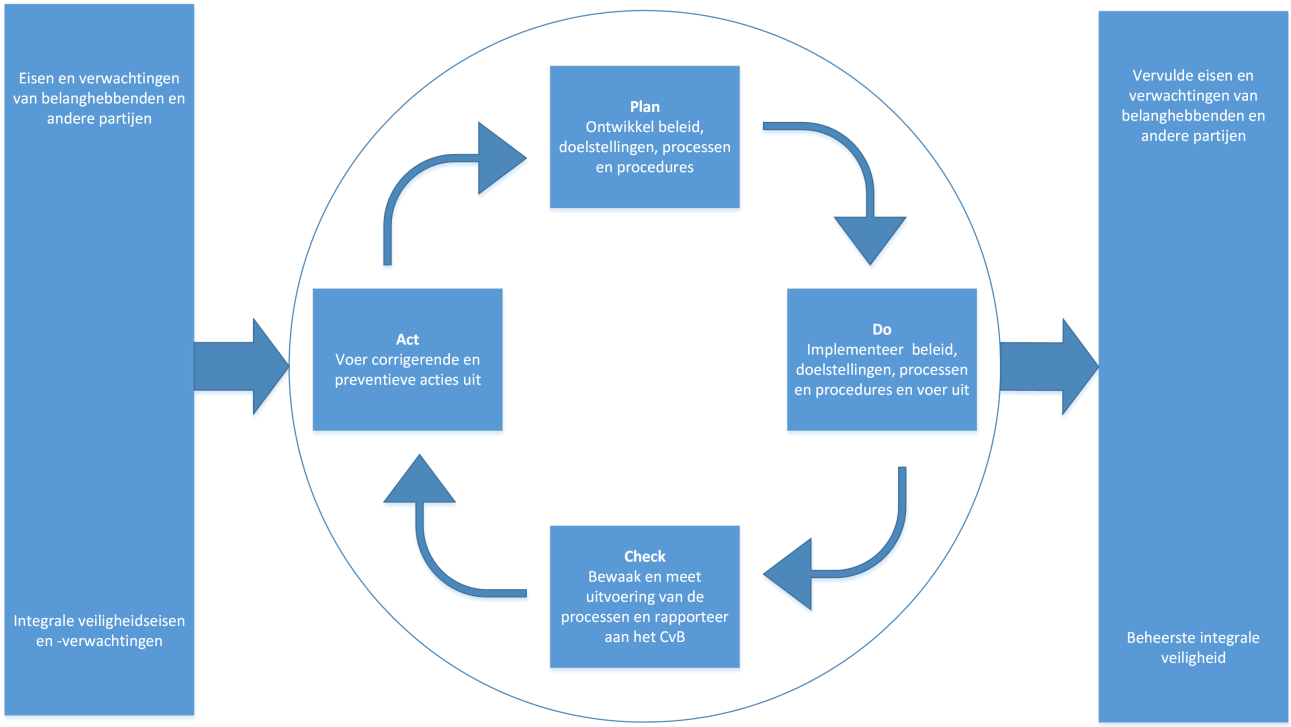
Dit inzicht kan worden opgebouwd door een vooronderzoek, met een GAP analyse dat resulteert in een startdocument voor besluitvorming. Het betreft een review om na te gaan in hoeverre de huidige werkwijzen voldoen aan criteria van het MIVH. Welke veiligheidsthema's en fasen van de PDCA-cyclus voldoen en welke hebben verbetering nodig. De review kan bestaan uit interviews, checklijsten, inspecties, audits en metingen.

In het vooronderzoek is in ieder geval aandacht voor de beleidsdoelstellingen, bedrijfsmiddelen, bedrijfsactiviteiten, producten en diensten van de instelling en hoe deze zich verhouden tot de missie van de instelling.
Daarbij moet het tevens helder zijn wat de afhankelijkheden zijn van de processen. Denk hierbij onder meer aan energie, ICT, kritieke hulpmiddelen en leveranciers.
Verder worden de veiligheidsrisico's geïdentificeerd. Let daarbij op dat ook de type risico's worden meegenomen voor niet-reguliere bedrijfssituaties. Identificeer de wet- en regelgeving en andere verplichtingen van de instelling, bijvoorbeeld rond contractonderzoek. Onderzoek ook de huidige risicomanagement praktijken en procedures, inclusief de activiteiten die door derden worden uitgevoerd en het kostenniveau. Ook geeft evaluatie van eerdere incidenten en non-compliance inzicht in de eigen organisatie en de noodzaak voor bepaalde risicobeheersing.

Daar waar relevant moet de juridische, politieke, culturele, sociale en economische factoren benoemd worden die van belang zijn voor het MIVH. Het moet helder zijn wat de essentiële processen en wat de essentiële klanten zijn. Het moet helder zijn wat normale en bijzondere omstandigheden en bedrijfsfuncties zijn. Belanfrijk is het om potentiële verstorende condities en incidenten te inventariseren. De relaties met de belangrijkste stakeholders (belanghebbenden) moeten benoemd inclusief hun risicoperceptie. Ook de normen die in de bedrijfstak vanzelfsprekend zijn, staan beschreven in het MIVH.

4.2 Behoeften en verwachtingen van partijen

Het MIVH is gericht op het beantwoorden van veiligheidsverwachtingen. Belanghebbenden hebben meestal verschillende behoeften. Een raad van bestuur zal vooral inzicht willen hebben in de mate van compliance, risicobeheersing en kosten. Individuele medewerkers, studenten en bezoekers hebben veelal meer behoefte aan sociale- en fysieke veiligheid.



Een heldere en afgestemde belanghebbenden analyse is essentieel om het MIVH in te richten en uit te voeren. Wie zijn belanghebbend op veiligheid in de instelling? Welke behoeften hebben besluitvormers, individuen in de organisatie, ketenpartners, opdrachtgevers, leveranciers en service partijen, vakbonden, individuen en groeperingen die beïnvloed worden door activiteiten van de instelling (bijvoorbeeld omwonenden), groeperingen van algemeen belang, financiers en verzekeraars, overheden en toezichthouders, hulpdiensten, media? Niet alle belanghebbenden hebben vanuit de instelling gezien eenzelfde impact. Met welke belanghebbenden moet expliciet afgestemd worden? Ook moet de instelling (management) kiezen in welke mate aan behoeften van belanghebbenden tegemoetgekomen wordt.

Een expliciete belanghebbendenanalyse is de grondslag om keuzes te maken in beleid, veiligheidsprogramma's en type maatregelen. Het is tevens de grondslag voor de communicatie met de doelgroepen. Deze communicatie kan bijvoorbeeld zijn gericht op de inrichting en implementatie van het MIVH, op bewustwording en training en op taken en verantwoordelijkheden tijdens een incident. Daarmee gaat een instelling gerichter in op de behoeften van de doelgroep en zal er voor het veiligheidsbeleid een grotere waardering ontstaan.

4.3 Reikwijdte van het MIVH

De reikwijdte van het MIVH wordt gevormd door de type risico's (veiligheidsthema's) die in eerste instantie tot het MIVH worden gerekend en de bedrijfsprocessen en -locaties waarvoor het MIVH van toepassing is.

Om te komen tot een goede scope afbakening is inzicht in de eigen organisatie belangrijk. Dit wordt opgebouwd in het onderdeel 'Instelling en zijn omgeving' (4.1) en 'Behoeften en verwachtingen van partijen' (4.2).

De reikwijdte van het MIVH moet zo helder mogelijk worden vastgelegd om het implementeerbaar te maken. De reikwijdte wordt altijd gevormd door een PDCA-cyclus bestaande uit de volgende elementen:

- opstellen van een adequaat operationeel integraal veiligheidsbeleid;
- identificeren van dreigingen voor het bepalen van de risico´s en impact;
- identificeren van wettelijke (en andere) vereisten;
- bepalen van prioriteiten en doelstellingen;
- het opstellen van een structuur en programma om het beleid en de doelen te realiseren;
- plannen, beheren, en monitoren van preventieve en reactieve maatregelen en het auditen hiervan om zeker te stellen dat de beleidsdoelstellingen gehaald worden en het veiligheidssysteem goed functioneert;
- in staat zijn om op veranderende omstandigheden in te spelen.

Het is ook mogelijk om het MIVH gefaseerd in te voeren. In deze situatie kan worden vastgelegd wat de reikwijdte is van de eerste fase en hoe de reikwijdte in de daarop volgende fasen wordt verbreed. Dit maakt het mogelijk om ervaringen op te bouwen, snel successen te communiceren en een beter inzicht te krijgen op bedrijfskritieke processen, compliance eisen en risico's.

5 Leiderschap

5.1 Leiderschap en betrokkenheid

Zonder actieve steun vanuit de top van de instelling is het niet mogelijk om een organisatiedoorsnijdend thema als veiligheid op een kwalitatief hoger niveau te organiseren. Er is meer nodig dan een plichtmatig akkoord op een beleidsvoorstel.

Valkuilen met betrekking tot management betrokkenheid
In de praktijk komt het vaak voor dat veiligheidsprojecten en activiteiten te laag in de organisatie worden gedelegeerd. Dit kan met zich meebrengen dat maatregelen geïsoleerd worden genomen en er onvoldoende integraliteit wordt bereikt. Een bestuurder mist dan informatie over de feitelijke risico's en rendement op veiligheidsaanpakken en de instelling kan geen verantwoording afleggen.

Ook komt het voor dat veiligheid belangrijk wordt gevonden en dat alles geregeld moet zijn, maar dat het niets mag kosten of dat alle projecten de hoogste prioriteit hebben en niemand tijd heeft. Soms is essentiële kennis alleen beschikbaar bij enkele sleutelfiguren. Of is deze kennis niet gedocumenteerd en zijn deze personen onvoldoende beschikbaar. Ook is er soms een gebrek aan interne deskundigheid om het MIVH te managen.

Verkrijgen van actieve steun van het bestuur
Actieve steun van het bestuur is essentieel voor het krijgen van voldoende budget voor veiligheidsmaatregelen en ook om doorzettingsmacht te krijgen op nieuwe werkwijzen rond veiligheid. Veiligheidsmaatregelen zullen alleen werken als deze ook worden gebruikt. Het voorbeeldgedrag door het bestuur, de 'tone at the top', is daarbij essentieel. Ook is het van belang dat het bestuur het gehele MIVH als 'big picture' ondersteunt en niet alleen afzonderlijke veiligheidsthema's of bepaalde veiligheidsmaatregelen. Het MIVH dient evenmin als een eenmalig project te worden beschouwd, maar als een continu proces dat onderdeel uitmaakt van de normale bedrijfsvoering.

Er zijn mogelijk twee aanvliegroutes om draagvlak voor een MIVH van het bestuur te krijgen. Het bestuur kan een kwaliteitsslag willen maken door een MIVH te implementeren, waarna de risico's beter beheersbaar zijn. Een andere route is dat de instelling al een veelheid aan eisen en risico's kent die beter beheersbaar moeten zijn en dat dit de reden is om een MIVH te implementeren. In het verlengde hiervan ligt ook het ontbreken van overzicht en het ontbreken van een gepaste accountability.

Voor het krijgen van actieve steun is het in ieder geval nodig dat de reikwijdte van het MIVH is afgestemd op de prioriteiten van het bestuur. De besluitvorming door het bestuur is op basis van een vooronderzoek, projectplan en kosten-baten analyse (business case). Het moet in ieder geval helder zijn wie van het bestuur betrokken is in het project, op welke wijze het bestuur haar steun uit voor het project en of er betrokkenheid nodig is van buiten de organisatie.

Afhankelijk van de scope en organisatorische context kun je het MIVH ook op afdelingsniveau invoeren, bijvoorbeeld in de laboratoria. Hiermee heeft in ieder geval dit organisatieonderdeel een systematische aanpak op de omgang met veiligheidsincidenten. De besluitvorming komt in dit geval bij het management van deze afdeling te liggen.

Business case (kosten/baten)
Het MIVH:

- verbetert de veiligheidsprestatie en risicobeheersing;
- vergroot compliance;
- versterkt de accountability op veiligheidsvraagstukken;
- zorgt ervoor dat instellingen verantwoord kunnen functioneren in onveilige omgevingen;
- vergroot de efficiency van processen (verlaging kosten);
- verbetert het vertrouwen en moraal bij medewerkers en studenten;
- verbetert het imago naar publiek, regelgevers en financiers;
- verbetert het veiligheidsbewustzijn.

De kosten van de invoering van een MIVH zijn vooral gerelateerd aan tijdsinvesteringen.

Projectplan
Het projectplan (implementatieplan) is gebaseerd op de resultaten van het vooronderzoek c.q. de GAP analyse. In het projectplan moet in ieder geval aandacht zijn voor de afbakening, de lange termijn doelstellingen ('stip aan de horizon'), korte termijn doelstellingen, de projectorganisatie, het ankerpunt naar het bestuur, de op te leveren resultaten, de uit te voeren activiteiten, de benodigde resources en budget, de momenten van afronding en de communicatie. Zie ook Bijlage 2 voor een mogelijk raamwerk van benodigde activiteiten voor invoering van een MIVH.

5.2 MIVH-beleid

Een MIVH-beleidsdocument moet worden opgesteld en vastgesteld door het bestuur. Zie 'NEN 7131 Maatschappelijke veiligheid – Managementsystemen voor veiligheid, voorbereiding op incidenten en continuïteit – Eisen en aanbevelingen' voor aspecten die opgenomen kunnen worden in de beleidsverklaring. Gedacht kan worden aan uitsluitingen, expliciete uiting van bestuursbetrokkenheid en de risicotolerantie van de organisatie. Daarnaast worden in die norm ook zaken behandeld zoals het eigenaarschap van het beleid, de formele acceptatie hiervan en het onderhoud van het beleid.

Het bestuurslid dat veiligheid in portefeuille heeft kan op gepaste bijeenkomsten 'op de zeepkist staan' om het beleid bekend te maken, waarna ook andere lijnmanagers dit kunnen doen. Ook zal het beleid via het intranet of externe website beschikbaar moeten zijn voor belanghebbenden, voor zover van toepassing.

5.3 Verantwoordelijkheden en bevoegdheden

Taken, verantwoordelijkheden en bevoegdheden moeten helder belegd zijn. Daarbij zijn er verschillende organisatorische invalshoeken.

Ten eerste zal er een organisatie zijn voor het integrale veiligheidsproces.

Veel instellingen beschikken nog niet over een integraal veiligheidsproces. De ontwikkeling en implementatie van het MIVH wordt dan het beste als een project georganiseerd. Het is nuttig om bij de bemensing van dit project al rekening te houden met de toekomstig staande organisatie van het veiligheidsproces. De toekomstig beheerder van het integrale veiligheidsproces kan dan al in de projectfase de documenten beheren en naar een vorm brengen die wenselijk wordt gevonden. Bijlage 2 bevat een raamwerk dat als basis voor het inrichten van een MIVH kan dienen. De ontwikkeling en implementatie van het MIVH op het niveau van een instelling kan aangepast worden aan de specifieke situatie en naar gelang de behoeften van de instelling georganiseerd worden.

Veiligheid wordt veelal in de lijn belegd als integrale managementverantwoordelijkheid. Daarbij moet het helder zijn wat decentrale verantwoordelijkheden en bevoegdheden zijn en welke dat zijn op centraal niveau. Processen worden vaak uitgevoerd op gezamenlijke locaties. Naast verantwoordelijkheid vanuit proceseigenaarschap zal er ook een locatiemanager zijn met verantwoordelijkheden en bevoegdheden op veiligheid.

Veiligheid heeft vele deelthema's. De coördinatie op ieder thema moet in de instelling belegd worden om inhoudelijke consistentie te krijgen. Daarnaast moet ook coördinatie tussen de thema's vorm krijgen.

Een vorm om de taken, verantwoordelijkheden en bevoegdheden helder te maken, is een zogenoemde RASCI-matrix, waarbij op de Y-as de relevante resultaten, processen en taken staan en op de X-as de actoren die een rol spelen in de veiligheidsaanpak. Bij iedere regel (resultaat, proces, taak) wordt daarna aangeven wie hierbij betrokken is en wat die betrokkenheid is (responsible, accountable, consulted, supported, informed).

Plan

Het MIVH kent een aantal activiteiten en resultaten die in de plan fase worden uitgevoerd c.q. bereikt.

6 Planvorming

6.1 Acties gericht op risico's en kansen

Een instelling voor Hoger Onderwijs heeft beperkte middelen. Een werkdag heeft slechts acht uur en een euro kan maar één keer worden uitgegeven. Hoe kan een instelling deze beperkte middelen over al haar beleidsterreinen verdelen? Veiligheid, samengebracht onder de noemer MIVH is slechts één van die domeinen. Ook binnen het MIVH kunnen de veiligheidsthema's concurreren om aandacht en middelen. Enerzijds bieden de missie en visie van de instelling alsmede de wensen en behoeften van belanghebbenden het kader waarbinnen de schaarse middelen worden verdeeld. Anderzijds geven wet- en regelgeving en normatieve referenties aan hoe die allocatie kan plaatsvinden. Het managen van risico's en het benutten van kansen stellen de instelling in staat haar doelen te bereiken. Het veiligheidsrisicomanagement is daarmee onderdeel van het risicomanagement van de gehele organisatie, ook wel Enterprise Risk Management (ERM). Overigens moet gerealiseerd worden dat er positieve en negatieve risico's bestaan die op een passende wijze op elkaar moeten worden afgewogen. Een risicoanalyse geeft inzicht in deze risico's en geeft een grondslag voor de te treffen maatregelen, de evaluatie op de getroffen maatregelen en voor de verantwoording van die keuzes.

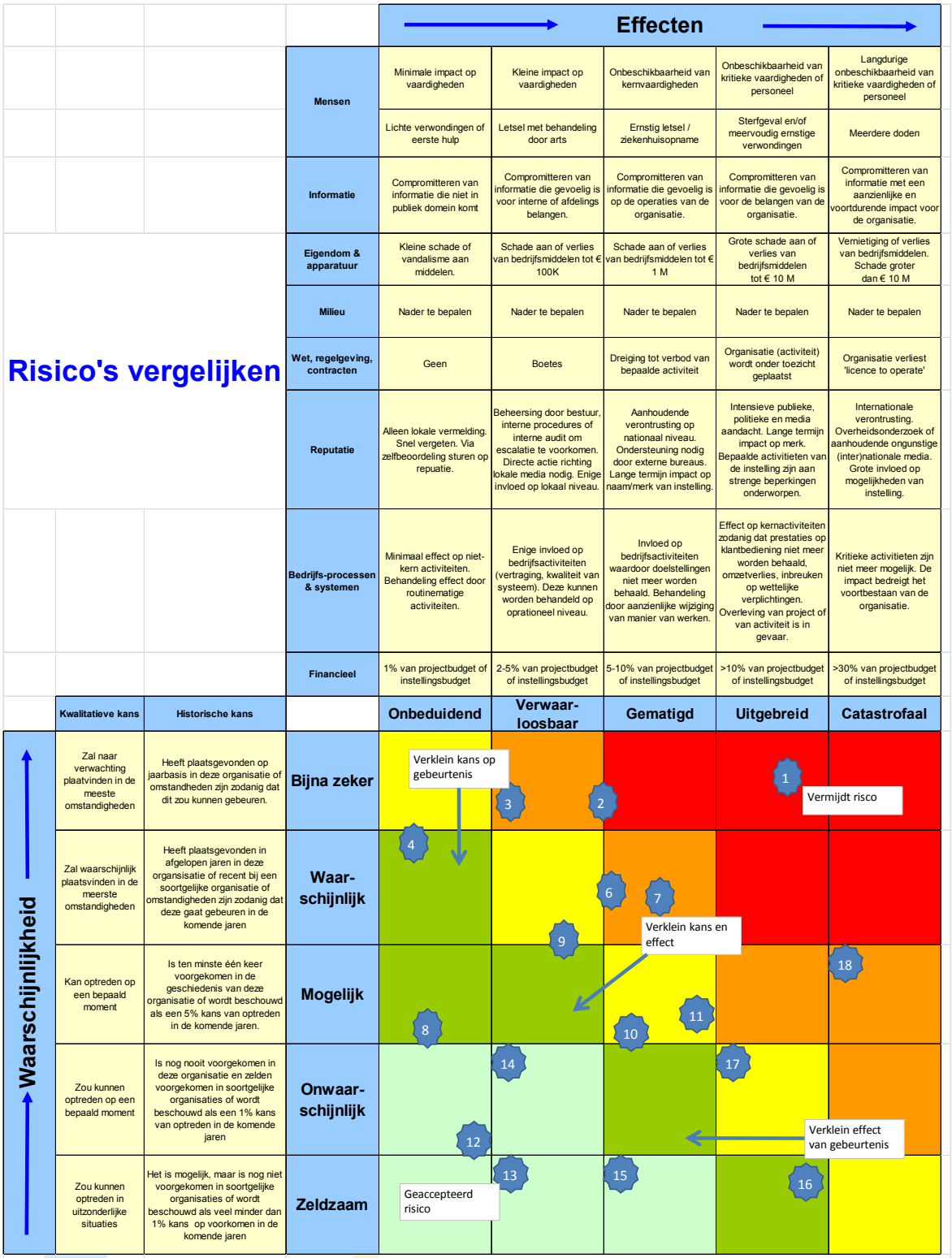
Het vergeven van middelen en manuren wordt in de instelling onderbouwd met de uitkomsten van risico en impact analyses. In die analyses wordt een afweging gemaakt tussen de belangen van de instelling en de mogelijke impact van verstoringen enerzijds en de waarschijnlijkheid van die verstoringen en kosten van risico-reductie anderzijds. In deze analyses dienen de belangen van de instelling en van haar belanghebbenden centraal te staan. Denk daarbij dat de verschillende beleidsterreinen, bijvoorbeeld onderwijs, onderzoek, bedrijfsvoering, huisvesting en personeelszaken, verschillende risico's met zich mee brengen.

Uitvoeren van risicoanalyse
Bij de start van een risicoanalyse is het belangrijk om de doelen van de instelling, de belangen van de stakeholders, het doel van de risicoanalyse en de scope duidelijk te hebben. Deze zijn in hoofdstuk 4 vastgelegd, maar mogelijk worden deze in de risicoanalyse verder verbijzonderd. Ook de risicoperceptie en risicoacceptatie worden in de inventarisatie meegenomen.

Vervolgens dienen de risico's van de instelling te worden benoemd en de belangrijkste risico's te worden geïdentificeerd. In het kader van de MIVH is het een uitdaging om voor alle veiligheidsthema's voldoende representatieve risico's te identificeren. Het inventariseren van de veiligheidsrisico's zou onderdeel van de belanghebbendenanalyse kunnen zijn, of een activiteit op zich. Een eerste risico-identificatie bestaat uit een tabel met te beschermen belangen en de mogelijke dreigingen hierop. Bijlage 3 bevat een dergelijke tabel op hoog niveau.
Vervolgens kan de mogelijke impact van een incident worden geschat en de waarschijnlijkheid dat een incident zal optreden.

Risico's vergelijken

			Effecten →				
			Onbeduidend	Verwaarloosbaar	Gematigd	Uitgebreid	Catastrofaal
		Mensen	Minimale impact op vaardigheden	Kleine impact op vaardigheden	Onbeschikbaarheid van kernvaardigheden	Onbeschikbaarheid van kritieke vaardigheden of personeel	Langdurige onbeschikbaarheid van kritieke vaardigheden of personeel
			Lichte verwondingen of eerste hulp	Letsel met behandeling door arts	Ernstig letsel / ziekenhuisopname	Sterfgeval en/of meervoudig ernstige verwondingen	Meerdere doden
		Informatie	Compromitteren van informatie die niet in publiek domein komt	Compromitteren van informatie die gevoelig is voor interne of afdelings belangen.	Compromitteren van informatie die gevoelig is op de operaties van de organisatie.	Compromitteren van informatie die gevoelig is voor de belangen van de organisatie.	Compromitteren van informatie met een aanzienlijke en voortdurende impact voor de organisatie.
		Eigendom & apparatuur	Kleine schade of vandalisme aan middelen.	Schade aan of verlies van bedrijfsmiddelen tot € 100K	Schade aan of verlies van bedrijfsmiddelen tot € 1 M	Grote schade aan of verlies van bedrijfsmiddelen tot € 10 M	Vernietiging of verlies van bedrijfsmiddelen. Schade groter dan € 10 M
		Milieu	Nader te bepalen	Nader te bepalen	Nader te bepalen	Nader te bepalen	Nader te bepalen
		Wet, regelgeving, contracten	Geen	Boetes	Dreiging tot verbod van bepaalde activiteit	Organisatie (activiteit) wordt onder toezicht geplaatst	Organisatie verliest 'licence to operate'
		Reputatie	Alleen lokale vermelding. Snel vergeten. Via zelfbeoordeling sturen op repuatie.	Beheersing door bestuur, interne procedures of interne audit om escalatie te voorkomen. Directe actie richting lokale media nodig. Enige invloed op lokaal niveau.	Aanhoudende verontrusting op nationaal niveau. Ondersteuning nodig door externe bureaus. Lange termijn impact op naam/merk van instelling.	Intensieve publieke, politieke en media aandacht. Lange termijn impact op merk. Bepaalde activitieten van de instelling zijn aan strenge beperkingen onderworpen.	Internationale verontrusting. Overheidsonderzoek of aanhoudende ongunstige (inter)nationale media. Grote invloed op mogelijkheden van instelling.
		Bedrijfs-processen & systemen	Minimaal effect op niet-kern activiteiten. Behandeling effect door routinematige activiteiten.	Enige invloed op bedrijfsactiviteiten (vertraging, kwaliteit van systeem). Deze kunnen worden behandeld op oprationeel niveau.	Invloed op bedrijfsactiviteiten waardoor doelstellingen niet meer worden behaald. Behandeling door aanzienlijke wijziging van manier van werken.	Effect op kernactiviteiten zodanig dat prestaties op klantbediening niet meer worden behaald, omzetverlies, inbreuken op wettelijke verplichtingen. Overleving van project of van activiteit is in gevaar.	Kritieke activitieten zijn niet meer mogelijk. De impact bedreigt het voortbestaan van de organisatie.
		Financieel	1% van projectbudget of instellingsbudget	2-5% van projectbudget of instellingsbudget	5-10% van projectbudget of instellingsbudget	>10% van projectbudget of instellingsbudget	>30% van projectbudget of instellingsbudget
Waarschijnlijkheid ↑	**Kwalitatieve kans**	**Historische kans**					
	Zal naar verwachting plaatvinden in de meeste omstandigheden	Heeft plaatsgevonden op jaarbasis in deze organisatie of omstandheden zijn zodanig dat dit zou kunnen gebeuren.	**Bijna zeker**				
	Zal waarschijnlijk plaatsvinden in de meerste omstandigheden	Heeft plaatsgevonden in afgelopen jaren in deze organsisatie of recent bij een soortgelijke organisatie of omstandigheden zijn zodanig dat deze gaat gebeuren in de komende jaren	**Waar-schijnlijk**				
	Kan optreden op een bepaald moment	Is ten minste één keer voorgekomen in de geschiedenis van deze organisatie of wordt beschouwd als een 5% kans van optreden in de komende jaren.	**Mogelijk**				
	Zou kunnen optreden op een bepaald moment	Is nog nooit voorgekomen in deze organisatie en zelden voorgekomen in soortgelijke organisaties of wordt beschouwd als een 1% kans van optreden in de komende jaren	**Onwaar-schijnlijk**				
	Zou kunnen optreden in uitzonderlijke situaties	Het is mogelijk, maar is nog niet voorgekomen in soortgelijke organisaties of wordt beschouwd als veel minder dan 1% kans op voorkomen in de komende jaren	**Zeldzaam**				



Zeer hoog (ZH)	Direct actie noodzakelijk vanuit het bestuur met gedetailleerde planning en monitoring
Hoog (H)	Hoog risico met aandacht vanuit senior management
Medium (M)	Management verantwoordelijkheid moet worden bepaald
Laag(L)	Monitoren van risico's and beheersbaar maken door routine procedures
Zeer laag (ZL)	Beheersbaar door routine procedures

Figuur 3 Veiligheidsrisico matrix[6]

[6] Afbeelding (deels) afkomstig van SRM BOK (zie bronnen).

Risico's vergelijken
Een Veiligheidsrisico Matrix visualiseert de spreiding van de risico's en prioriteert risico's. Veel gebruikt worden matrices van 5x5 (mogelijke impact en waarschijnlijkheid) waarbij binnen de matrix vier of vijf risiconiveaus zijn aangegeven. Soms worden de risiconiveaus juist niet geclassificeerd om de indruk van wiskundige precisie en nauwkeurige inschatting van risico's weg te nemen.

Voor een voorbeeld van zo een matrix zijn in de voorgaande figuur 18 risico's geplot.

De getoonde matrix scoort de risico's op de effectsoorten Mensen/vaardigheden, Mensen/letsel, Informatie, Eigendom & Apparatuur, Milieu, Vergunningen, Reputatie, Financiën en Bedrijfsprocessen. De matrix is een eerste voorzet op de criteria en in het beleidstraject van de instelling kunnen deze criteria verder worden besproken en vastgesteld.
Een gebeurtenis heeft één waarschijnlijkheid en kan verschillende type effecten hebben in verschillende effecthoogten. Bij het bepalen van de hoogte van het risico is het gebruikelijk om de hoogste effecthoogte te gebruiken.

Risico behandeling
Met kleuren kan het risicobeleid van de instelling tot uitdrukking worden gebracht. In het voorbeeld van de matrix zijn risico's in het rood nimmer acceptabel en zijn risico's in de blauwe en groene vakken de geaccepteerde risico's. De risico's in de gele en oranje vakken dienen bijzondere managementaandacht te hebben.

Prioriteiten in het aanpakken van risico's kunnen zijn: de risico's met de hoogste impact, met de hoogste waarschijnlijkheid en/of risico's met het hoogste product van impact X waarschijnlijkheid.

In de risicobehandeling kan gekozen worden voor risicobeheersing of voor risicofinanciering.
Risicobeheersing richt zich operationeel op het risico en bestaat uit de volgende opties:

- Terminate (voorkomen). Hierbij wordt gestopt met een risicovolle activiteit, waarna het risico niet meer bestaat.
- Treat (verminderen). Hierbij kan gekozen worden op maatregelen die de kans op een incident verkleinen (= preventie) of op maatregelen die de impact van een incident verkleinen.

Risicofinanciering kent de volgende opties:

- Transfer (overdragen). Hierbij wordt het financiële risico overgedragen naar de klant, leverancier, verzekeraar of overheid.
- Take (accepteren). Hierbij wordt het risico geaccepteerd en het verlies gebudgetteerd.

Risicofinanciering is vooral bruikbaar voor financiële risico's. Voor andere type effecten, denk aan beperking van letselschade of reputatieschade, is deze ongeschikt. Het stoppen van risicovolle activiteiten is vaak niet mogelijk, omdat deze vaak samenhangen met de kern van de bedrijfsactiviteit.

Dit houdt in dat vooral gestuurd kan worden op operationele vermindering van het risico. In principe is preventie het fundament om de risico's te verkleinen. Met preventie wordt de kans verkleind dat een risicovolle gebeurtenis kan plaatsvinden of zich tot een groter incident kan ontwikkelen. Daarnaast horen er maatregelen te zijn om het incident te bestrijden en om de effecten van het incident te verkleinen.

Bij de risico evaluatie moet ook gekeken worden naar de kosten van de risicovermindering. Dit kunnen financiële kosten zijn maar ook organisatorische lasten. Sommige hogere risico's zijn alleen tegen onevenredig hoge kosten te verlagen. De doelstelling op het gewenste risiconiveau zou dan 'ALARP'

kunnen zijn. Dit staat voor ‘As Low As Reasonably Practical’ en betekent dat een kosteneffectief risiconiveau wordt nagestreefd.

Risicoregister
In de instelling zullen vele risico’s geïdentificeerd zijn. Het is daarna praktisch om de belangrijkste risico’s in een register te plaatsen met in ieder geval de waarschijnlijkheid en impact van dat risico en de verantwoordelijke persoon binnen de instelling op de verdere omgang met dit risico. Dit register kan daarna uitgebreid worden met de belangrijkste controls op dit risico, het restrisico en de nog te implementeren maatregelen.

Normen en good practices:

- NEN-ISO 31000 Risicomanagement – Principes en richtlijnen. Dit is een raamwerk en proces voor het beoordelen en managen van risico’s. Het is bedoeld voor enterprise risk management. De instelling kan op basis van deze referentie zowel de veiligheidsrisico’s als andere risico’s van de organisatie managen.
- NEN-ISO/IEC 31010:2009 Risico management - Risico-evaluatie technieken. Dit betreft een overzicht van bruikbare technieken om risico’s te beoordelen.
- ISO/IEC 27005:2014 Information technology -- Security techniques -- Information security risk management gaat in op risicomanagement met betrekking tot informatiebeveiliging.
- Risico-inventarisatie & Evaluatie (RIE). Dit is het instrument om risico’s op arbeidsomstandigheden in kaart te brengen.

6.2 MIVH-doelen en hoe deze worden bereikt

De doelen van het MIVH moeten helder zijn. Deze worden gevormd uit het MIVH-beleid (zie 5.2) en de risicoanalyse (zie 6.1), de wettelijke eisen, overige eisen en uit wensen en eisen van belanghebbende partijen (zie 4.2).

Een voorbeeld van een doel is dat veiligheid van personen altijd prioriteit heeft.

In de voorbereidende fase horen de wettelijke eisen en de overige eisen al op hoog niveau geïdentificeerd te worden. In de planfase wordt dit verder uitgewerkt. Maak een register met wettelijke eisen en overige eisen en zorg voor een actuele en voor medewerkers toegankelijke procedure . In de praktijk ontbreekt dit vaak. Dan wordt pas in de check-fase een analyse gemaakt op de regelgeving die van toepassing is. Zie paragraaf 9.4 voor een aanpak op toetsing op wettelijk kader.
Voorbeelden van overige eisen zijn overeenkomsten met overheidspartijen, contracten met klanten, overeenkomsten met andere partijen, branchecodes en publieke toezeggingen van de raad van bestuur. Overige eisen kunnen ook gericht zijn op de architectuur van maatregelen en het kostenniveau. Denk bijvoorbeeld aan de wenselijkheid van één ID/toegangskaart voor alle betrokkenen van de instelling die bruikbaar is voor fysieke toegang, logische toegang en andere vormen waarbij ID wenselijk is.

Deze eisen kunnen daarna worden vertaald naar MIVH-doelen (‘objectives’) consistent aan het beleid van de organisatie. Daarna dienen deze doelen meetbaar gemaakt te worden (‘targets’). Het plannen van

het bereiken van de doelen van het MIVH zal zo SMART[7] mogelijk worden geformuleerd. Daarbij zal ten minste worden vastgesteld:

- wat dient te gebeuren;
- welke middelen daarvoor nodig zijn;
- wie voor de uitvoering verantwoordelijk is. Dit kan bijvoorbeeld gedaan worden via een RASCI-tabel;
- wanneer het volbracht dient te zijn;
- hoe de resultaten dienen te worden beoordeeld. Wie beoordeelt en aan de hand van welke criteria.

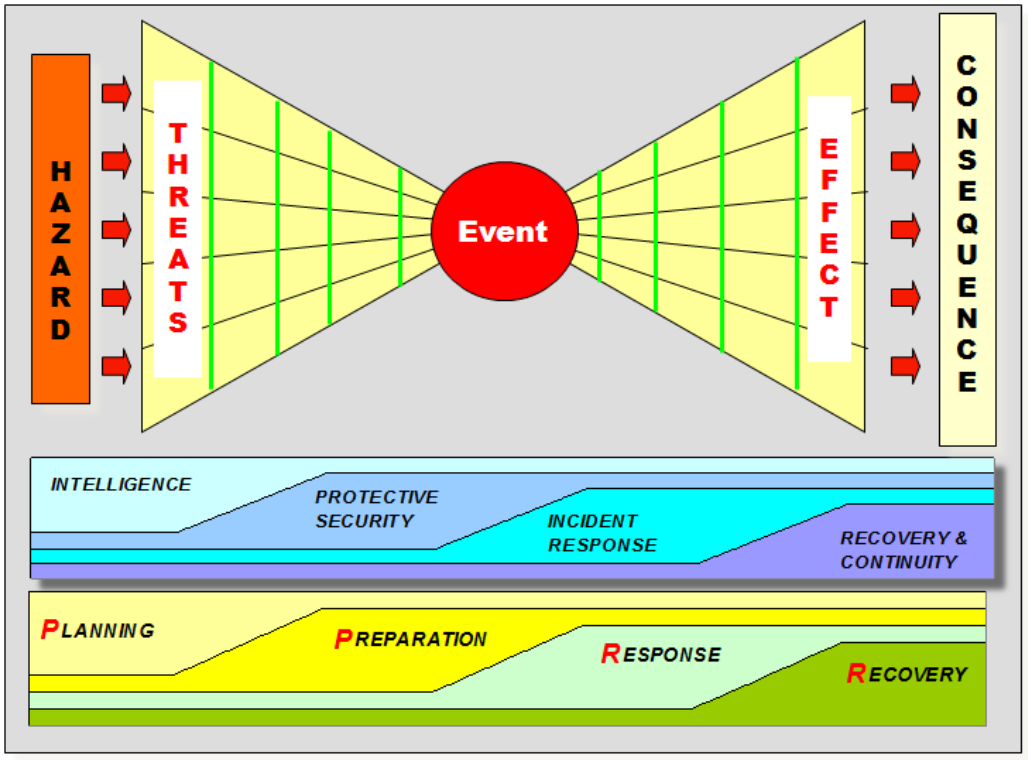
Een aanpak op het plannen van doelen en acties van het MIVH is opgenomen in bijlage 2.

Veiligheidsdoelen kun je ook aan veiligheidsthema's koppelen. Per thema kan daarna verder invulling aan de doelen worden gegeven. De volgende veiligheidsthema's staan centraal in deze handleiding voor MIVH: Arbeidsomstandigheden, Milieuveiligheid, Sociale veiligheid, Integriteit, Informatieveiligheid, Privacy, Kennisveiligheid, Internationalisering, Gebouwveiligheid, Crisismanagement. In hoofdstuk 8 wordt nader ingegaan op deze thema's en bijlage 3 geeft naast voorbeelden van relaties tussen dreigingen en te beschermen belangen, ook relaties tussen veiligheidsthema's en type dreigingen en veiligheidsthema's en te beschermen belangen.

Een bruikbare aanpak is het stellen van doelen in de veiligheidsketen. Sommige risico's worden verkleind door een andere inrichting van het bedrijfsproces. Dit wordt pro-actie genoemd. Ook kunnen preventieve maatregelen worden getroffen om de kans op het optreden van een verstorend incident te verkleinen. De omgang met brand, technisch/organisatorisch en menselijk falen en ook de omgang met natuur- en omgevingsdreigingen wordt safety genoemd. De omgang met moedwillig wederrechtelijk handelen is security[8]. Het voorbereid zijn op een verstorend incident wordt preparatie genoemd en het acteren op of tijdens dat incident is de response. De response bestaat uit de incidentbestrijding om de gevolgen van het incident te beperken. Denk hierbij aan BHV, maar ook aan een (digitale) brandweer, salvage en ook crisiscommunicatie en crisisorganisatie. Door een incident kan het bedrijfscontinuïteitsplan worden geactiveerd dat moet zorgen dat de essentiële bedrijfsfuncties in enige mate voortgezet kunnen worden en dat de situatie hersteld kan worden.

Per type risico moet worden aangegeven waar de zwaartepunten van de maatregelen komen te liggen. Wordt vooral ingezet op maatregelen om een dreiging in een vroegtijdig stadium te onderkennen, op preventieve maatregelen waardoor een dreiging minder eenvoudig tot een incident leidt, op response/bestrijding of op bedrijfscontinuïteit en herstel na een incident? Dit kan ook helder worden gemaakt in een zogenoemde Bow-Tie diagram. Zie figuur 5.

[7] SMART is Specifiek, Meetbaar, Acceptabel, Realistisch, Tijdgebonden
[8] Sommige veiligheidsdomeinen zijn vooral gericht op security, andere veiligheidsdomeinen zijn vooral op safety gericht. Informatiebeveiliging richt zich op beiden en maakt niet een sterk onderscheid tussen safety en security.



Figuur 5 Bow Tie diagram[9]

7 Ondersteuning

7.1 Middelen

Ontwerp, implementatie en uitvoering van een managementsysteem voor integrale veiligheid behoeft de allocatie en toewijzing van voldoende mankracht en financiële middelen.

Op alle niveaus en binnen nagenoeg alle afdelingen van de instelling dienen medewerkers te worden belast met taken en verantwoordelijkheden voor het beheersen van veiligheidsrisico's. Het bestuur dient de visie en het beleid voor MIVH te onderschrijven en op implementatie en naleving toe te zien. Daartoe moeten functionarissen worden aangewezen die dit beleid operationaliseren. De doelstellingen op dit beleid zijn in hoofdstuk 6.2 geoperationaliseerd. Experts worden voor de verschillende veiligheidsthema's ingezet om risicoanalyses uit te voeren, kwetsbaarheden in kaart te brengen en verbetervoorstellen te formuleren. Alle medewerkers dienen naar vermogen bij te dragen aan het MIVH van de instelling.

Organisatorische structuren en procedures dienen te zijn opgesteld om veiligheidsincidenten het hoofd te bieden en om een crisis te kunnen managen. Een crisisorganisatie met eenduidige verantwoordelijkheden en bevoegdheden dient te zijn ingericht, en te worden geoefend. Verschillende onderdelen en disciplines van de instelling zijn vertegenwoordigd in of aangesloten bij het crisisteam, zoals bestuur, communicatie, juridisch, faculteiten, HRM, ICT en facilitair.

[9] Figuur afkomstig uit SRM BOK.

Voor specifieke veiligheidsincidenten kunnen responsteams worden samengesteld en getraind. Hiervoor dienen toegesneden plannen en procedures te worden opgesteld. Voorbeelden van responsteams zijn Bedrijfshulpverlening (BHV) voor hulpverlening bij calamiteiten in gebouwen, Computer Emergency Respons Team (CERT) voor hulp bij ernstige computerstoringen en Steunpunt Studenten in Nood voor hulp aan studenten in het buitenland.

7.2 Competenties

Op alle niveaus in de instelling zijn medewerkers belast met taken, bevoegdheden en verantwoordelijkheden voor MIVH. Dit wordt vastgelegd in hoofdstuk 5.3.

Het is zinvol om de veiligheidstaken vast te leggen in functieprofielen. Dan kunnen ook de noodzakelijke competenties worden beschreven en is het sturen op ontwikkeling en behoud van die competenties eenvoudiger. Er moet voldoende tijd en middelen beschikbaar zijn voor continue scholing op veiligheid. In functioneringsgesprekken en beoordelingen dienen ook deze competenties te worden meegewogen.

7.3 Bewustzijn

Veel veiligheidsincidenten kennen een oorzaak in menselijk handelen. Onbekendheid met een risico of met veiligheidsmaatregelen, nalatigheid, organisatorisch en menselijk falen kunnen een veiligheidsgebeurtenis veroorzaken en verergeren. De mens kan de zwakste schakel zijn, maar ook een hele sterke schakel zijn in het signaleren van een (naderend) veiligheidsincident en het bestrijden van dat incident.

Het planmatig sturen op bewustzijn is een effectieve manier om de risico's te beperken. Een bewustzijn programma is doelgroep gericht. Een eerste stap is om voldoende kennis over te brengen bij de doelgroepen. Wat zijn de risico's, waarop te letten en wat is de eigen rol bij een incident of bij het voorkomen van een incident? Via metingen kan gecontroleerd worden of er in de doelgroepen voldoende kennis aanwezig is of dat er opnieuw aandacht op deze onderwerpen gevestigd moet worden. Over langere periode kan een cultuur ontstaan waarbij het gewenste gedrag wordt getoond. Hierbij is het noodzakelijk dat leidinggevenden het voorbeeldgedrag tonen ('tone at the top'), er een cultuur is waarbij personen elkaar kunnen aanspreken op het gedrag en dat het gewenste gedrag ook geoefend wordt.

Startpunt is in ieder geval om voldoende kennis over te brengen. Medewerkers en studenten dienen zich bewust te zijn van de veiligheidsrisico's die werken, studeren en onderzoek met zich meebrengen. De instelling zal voortdurend de aandacht moeten vestigen op het bestaan van en het omgaan met deze risico's. Dit kan de instelling bereiken via bijvoorbeeld in een startgesprek bij kennismaking met de instelling op de eerste werk- of studiedag, instructies over specifieke veiligheidsprocedures, veiligheidsvideo's, brochures, functioneringsgesprekken, posters, incidentevaluaties en lezingen.

Het project integrale veiligheid hoger onderwijs heeft een deelproject op bewustwording.

7.4 Communicatie

De werking van het MIVH is afhankelijk van een goede communicatie. Hiervoor is een plan nodig, communicatiemogelijkheden en communicatieprocedures.

Er is communicatie nodig met betrekking tot de management structuur. Maak hierbij onderscheid op communicatie op strategisch niveau, tactisch niveau en operationeel niveau. In hoofdstuk 4.2 is vastgelegd wie de belanghebbenden zijn bij het MIVH en wat de behoeften zijn. Hierop kan gericht gecommuniceerd worden. Grote doelgroepen als medewerkers en studenten kunnen geïnformeerd worden via bijeenkomsten, werkgroepen, nieuwsbrieven en intranet op de veiligheidsthema's, de doelstellingen en de structuur en werkwijze van het MIVH.

Daarnaast is er communicatie met betrekking tot veiligheidsthema's en type incidenten. Daarbij onderscheiden we communicatie in de proactieve fase (koude fase), tijdens een crisis en na afloop van een incident.

Afstemming en communicatie met de buitenwereld dient ook te worden geborgd. Zowel onder normale omstandigheden als bij een veiligheidsincident of een crisis beheert de instelling een netwerk van externe partijen. De samenwerking met externe partijen kan op verschillende vlakken en op verschillende momenten in de veiligheidsketen geschieden. Bijvoorbeeld het verkrijgen van dreigingsinformatie en waarschuwingen over tendensen van radicalisering, of het preventief optreden bij een groot evenement, of de respons op een brandmelding en de nazorg bij een calamiteit. Afhankelijk van de aard en omvang van de instelling en de aard van het veiligheidsdomein zijn relaties nodig met bijvoorbeeld de gemeente, politie, brandweer, veiligheidsregio, NCTV of AIVD. Goede werkafspraken zijn essentieel, al dan niet gezamenlijk, in de regio of met landelijke platforms of communities of practice.

De doelstellingen, werkwijze en middelen voor de in- en externe communicatie worden in procedures vastgelegd. Daarin kan ook het proces zijn beschreven over wie met wie, wanneer, hoe en met welke frequentie communiceert.

De communicatieprocedure MIVH dient naast normale omstandigheden ook de communicatie bij incidenten en tijdens crises te voorzien. Het voorbereiden van communicatieprotocollen, draaiboeken, het trainen van de woordvoerder en het afstemmen en oefenen van crisiscommunicatie verdient extra aandacht.

7.5 Gedocumenteerde informatie

De opzet en werking van het MIVH moet zijn beschreven en gedocumenteerd. Dan gaat het vooral om: de toebedeelde verantwoordelijkheden, de samenhang tussen veiligheidsthema's, de methode van risicoanalyse en de besluiten over omgaan met non-conformiteiten en risico's.

Voorbeelden van MIVH documenten zijn: beleidsdocumenten, organigrammen, planningen met doelstellingen, risico- en impactanalyses, procedures en processen, normen, handleidingen, crisisplannen, en evaluatie, review en audit rapporten. Het afleggen van verantwoording in bijvoorbeeld afdelingsverslagen en jaarrapportages en het aantonen van 'compliance' en 'governance' zijn ook voorbeelden van MIVH documenten.

Do

De zogenoemde ‘do fase’ van de managementcyclus bevat de implementatie en werking van de veiligheidsmaatregelen.

Na een inleidende paragraaf (8.1) worden de tien veiligheidsthema’s kort besproken. De huidig bekende normen en handreikingen op die veiligheidsthema’s zijn in bijlage 1 vastgelegd.

8 Werking

8.1 Operationele planvorming en beheersing - algemeen

De instelling moet processen plannen, implementeren en beheersen die nodig zijn om de acties uit te voeren die voortkomen uit de eerder geschetste risicoanalyses. Ook kunnen acties voortkomen uit management reviews en onderzoeken (audits) die ‘non-conformiteiten’ hebben blootgelegd. Zie hiervoor hoofdstuk 9.

Voor de goede uitvoering van die verbeterprocessen dienen criteria te worden vastgesteld die SMART geformuleerd zijn. Hierbij zijn ook KPI’s (kritieke prestatie indicatoren) bruikbaar.

Het beheer en aansturing van die processen en de documentatie daarvan, beoogt dat de processen worden uitgevoerd zoals gepland en dat hierover verantwoording kan worden afgelegd.

De instelling zal de (neven)effecten van geplande wijzigingen en de gevolgen van ongeplande wijzigingen evalueren en beoordelen. Waar nodig zullen nieuwe verbeteracties worden uitgevoerd om negatieve (neven)effecten en gevolgen te mitigeren.

De instelling zorgt ervoor dat ook uitbesteedde processen worden beheerst.

In de volgende secties van dit hoofdstuk zijn de veiligheidsthema’s die spelen binnen een instelling voor Hoger Onderwijs kort beschreven. Per thema wordt na een korte introductie een aantal mogelijke risico’s geschetst en een suggestie gedaan van mogelijke beheersmaatregelen die kunnen worden getroffen en welke normatieve kaders daarbij een rol kunnen spelen.

8.2 Arbeidsomstandigheden

Een instelling voor Hoger Onderwijs is ook werkgever in de zin van de Arbeidsomstandighedenwet. Deze wet is overigens ook van toepassing op de zorg voor studenten. Medewerkers, onderzoekers en studenten zijn aangewezen op de door de instelling gefaciliteerde arbeidsomstandigheden.

De instelling zal alles in het werk stellen om ongevallen en lichamelijk letsel in de instelling te vermijden. Deze kunnen worden veroorzaakt door bijvoorbeeld gladheid of andere niet-stabiele ondergrond, omvallende objecten, maar ook door gebruik van speciale machines, gebruik van ongekeurde elektrische handgereedschappen en toestellen en blootstelling aan hoge voltages, dampen, stralingen, bacteriën of virussen. Een gezonde werkplek met voldoende licht, goed klimaat en aandacht voor goede werkhouding kan RSI en andere lichamelijke klachten voorkomen. Risicovolle locaties dienen te worden afgeschermd

voor onbevoegden, gecontroleerde toegang en heldere gedragsregels, trainingen en voorlichting moeten de veiligheid van deze locaties verhogen.

De interne rechtsbescherming voor studenten is geregeld in de WHW. Zo dienen instellingen in het hoger onderwijs te beschikken over een faciliteit, één loket waar studenten terecht kunnen als ze klachten hebben. Daarnaast moet iedere instelling beschikken over instrumenten als een klachtenregeling, ombudsman voor personeel, een regeling ongewenst gedrag, integriteitscode en een klokkenluidersregeling.

Werkstress en ongewenst gedrag kan psychosociale schade veroorzaken. Aandacht hiervoor en voor arbeidsverzuim in de breedte is belangrijk om hierop grip te krijgen. De Arbocatalogus van VSNU en VH besteden aandacht aan psychosociale arbeidsbelasting van medewerkers.

8.3 Milieuveiligheid

Het beschermen van het milieu en het inrichten van een duurzame samenleving heeft een hoge prioriteit binnen de instelling. Per instelling kunnen de uitdagingen hier sterk verschillen. Laboratoria met proefdieren zullen bijvoorbeeld aandacht van dierenrechten activisten willen vermijden. Een instelling met een onderzoeksreactor zal radiologische en nucleaire besmettingen willen voorkomen en het beheer van splijtstoffen willen zekerstellen.
Naast duurzaamheid speelt hier het behouden van vergunningen een belangrijke rol. Het primaire proces van de instelling is direct met die ‘licence to operate’ verbonden. Bovendien kunnen incidenten leiden tot ernstige imago schade, hoge boetes, oplopende schoonmaak en herstelkosten en schadeclaims.
Milieuveiligheid kent diverse aandachtspunten. De energiebelasting wordt vooral veroorzaakt door verwarming, koeling en verlichting. Het afval wordt bepaald door herbruikbaarheid, scheiding van afvalstromen en belasting van riolering en oppervlaktewater. Op locaties met warmwater kan zich legionella nestelen en in oudere gebouwen kan nog asbest voorkomen.
Op bijzondere locaties van de instelling kunnen gevaren voor mens en milieu ontstaan vanuit aanwezigheid en gebruik van chemicaliën, gen-manipulatie, radiologische activiteiten en nucleaire activiteiten. Ook het gebruik van proefdieren in diervriendelijke omstandigheden kan tot dit beleidsterrein worden gerekend.
De verschillende milieuvergunningen worden gebundeld in de omgevingsvergunning. Iedere instelling zal in ieder geval een milieufunctionaris moeten hebben voor coördinatie op dit beleidsterrein. Indien er radioactieve straling mogelijk is, zal de instelling ook een radiologische/stralingsfunctionaris moeten hebben die tevens de beveiliging op deze bronnen coördineert. Wanneer de instelling biologische laboratoria heeft, moet een biologische veiligheidsfunctionaris (BVS) zijn aangesteld die tevens de beveiliging coördineert.

8.4 Sociale veiligheid

Bij een instelling voor Hoger Onderwijs werken, studeren en onderzoeken mensen in uiteenlopende omstandigheden met elkaar. Het waarborgen van de sociale veiligheid van die mensen is een belangrijke verantwoordelijkheden van de instelling. Mensen moeten zich veilig voelen en hun lichamelijke en geestelijke integriteit moet gewaarborgd zijn. Ook de veiligheid van persoonlijke eigendommen draagt bij aan de sociale veiligheid. Die sociale veiligheid wordt gewaarborgd in de gebouwen en op de terreinen van de instelling. Maar de verantwoordelijkheid strekt zich verder uit dan dat. Denk bijvoorbeeld aan de sociale veiligheid bij huisvesting, sociale omgang en tijdens studiereizen. De instelling zal alert zijn en

maatregelen moeten treffen om sociale onveiligheid zoals pesterijen, seksuele intimidatie, diefstal van persoonlijke eigendommen en bedreiging van medewerkers te voorkomen.

Doordat instellingen een afspiegeling vormen van de maatschappij worden ook zij geconfronteerd met maatschappelijke ontwikkelingen. Hiertoe behoren ook het gebruik van geweld door eenlingen en radicalisering. De instellingen bevinden zich daar op het snijvlak van maatschappelijk, persoonlijk en instellingsbelang. Dit vraagt om behoedzaam en tactvol opereren.

8.5 Integriteit

Behoefte aan moreel kompas
Integriteit vormt de hoeksteen van professioneel handelen. Het is een kernwaarde van en drijfveer voor professionals, in alle sectoren van de samenleving. Mensen koersen op hun moreel kompas om vanuit een intrinsieke motivatie de goede dingen te doen en de dingen goed te doen. Naast deze interne factoren spelen bij de uitvoering van werkzaamheden ook externe prikkels een rol. Soms ontstaat een onbalans tussen intrinsieke en extrinsieke motivatie waardoor het moreel kompas van slag kan raken. De morele balans tussen wat 'wel' en niet (meer)' door de beugel kan, raakt ontregeld. Dan is er mogelijk sprake van integriteitschending. Op verschillende plekken duiken kwesties op die duiden op gebrek aan integer handelen, recent ook rondom voorheen betrouwbaar geachte sectoren in de samenleving. Incidenten bij banken, woningcorporaties, ziekenhuizen, onderwijsinstellingen en wetenschap leiden tot maatschappelijke verontwaardiging en geschonden vertrouwen.

Voorkomen is beter dan genezen
Beschadigd vertrouwen laat zich niet altijd vanzelfsprekend herstellen en vraagt vaak veel tijd en energie. In onze samenleving speelt vertrouwen een belangrijke rol, zo ook in het hoger onderwijs en onderzoek. Het bepaalt in hoge mate hoe we tegen elkaar aan kijken en hoe we met elkaar omgaan.
De remedie voor herstellen van vertrouwen is voorkómen. Tijd om stil te staan bij waar het eigenlijk om gaat bij integriteit in het hoger onderwijs. Het hoog houden en garanderen van kwalitatief goed en betrouwbaar onderwijs en onderzoek is een verantwoordelijkheid die betrokkenen, studenten, medewerkers en bestuurders alleen samen kunnen waarmaken. Aandacht voor integriteit, professioneel en wetenschappelijk, is daarbij cruciaal. De samenleving moet kunnen vertrouwen op een goed functionerende instelling voor Hoger Onderwijs. Professionaliteit, betrouwbaarheid, onkreukbaarheid en zorgvuldigheid dragen bij aan dit vertrouwen. De integriteit van de sector als geheel is daarbij afhankelijk van de integriteit van iedere medewerker, bestuurder, docent en student.

De sector kent diverse praktijkvoorbeelden op schending van integriteit. Doorgaans trekken deze incidenten veel media-aandacht en veroorzaken zij reputatieschade.

Een instelling voor Hoger Onderwijs kan veel doen om de integriteit van bestuurders, docenten, onderzoekers, medewerkers en studenten te waarborgen. Een gedragscode waarin de omgang met dilemma's en normen voor afwijkend gedrag zijn beschreven, is een eerste en belangrijke aanzet daartoe. Andere voorbeelden van integriteitsmaatregelen zijn het aanwijzen van vertrouwenspersonen, een gedragsnorm goed bestuur en integriteit en maatregelen om examen- en tentamenfraude tegen te gaan.

8.6 Informatieveiligheid

De hele samenleving en ook een instelling voor Hoger Onderwijs is steeds meer afhankelijk van computers, internet, smartphones en allerlei digitale applicaties. In feite kunnen we niet meer zonder, niet als persoon, niet als instelling en niet als maatschappij. Informatieveiligheid gaat over het beschermen en borgen van deze digitale voorzieningen. De complexiteit van de ICT-infrastructuur (netwerken, providers, Cloud), hardware (laptops, tablets, servers, mobiele devices), besturingssystemen (MS-DOS, Linux, iOS) en ontelbare software pakketten en applicaties maken dit een buitengewoon ingewikkeld vakgebied met vele disciplines en expertisegebieden.

Een groot risico van tekortschietende informatieveiligheid kan zijn: geen beschikbaarheid van ICT infrastructuur en daardoor geen toegang tot de eigen informatie. Daarnaast kunnen diefstal van ICT-apparatuur en het verlies van grote hoeveelheden informatie tot aanzienlijke schadeposten leiden. Gecorrumpeerde databases en onbetrouwbare bewerkingen van onderzoeksgegevens, bedrijfsvoering gegevens en studentenadministraties kunnen voor veel problemen zorgen. Maar ook in het hoger onderwijs ligt digitale fraude, schending van de privacy van studenten en medewerkers en boetes vanwege het niet voldoen aan wet- en regelgeving op de loer. Ook schadeclaims bijvoorbeeld bij contractonderzoek en schending van intellectueel eigendom zijn niet uit te sluiten.

Een instelling voor Hoger Onderwijs moet investeren om de risico's van ICT-falen en Cybercrime zo goed mogelijk te beheersen. Het formuleren van beleid, het opstellen van meerjarenplannen en het inzetten van experts is daarbij onontbeerlijk. Een veel gebruikt normenkader is ISO 27002. Dit normatieve document bestaat uit de volgende hoofdstukken: Beveiligingsbeleid, Organisatie van informatiebeveiliging, Personele maatregelen, Beheer van ICT-middelen, Logisch toegangsbeheer, Cryptografie, Fysieke beveiliging en beveiliging van de omgeving, Operationele beveiliging, Beveiliging van de communicatie, Acquisitie en ontwikkeling en beheer van ICT-middelen, Leverancier relaties, Incident management, Bedrijfscontinuïteit van ICT-middelen, Naleving. SURF heeft onder andere op dit normenkader verschillende handreikingen voor instellingen voor hoger onderwijs ontwikkeld. Zie bronnen (bijlage 1-5).

8.7 Privacy

Een instelling voor hoger onderwijs gebruikt vanzelfsprekend persoonsgegevens in tal van processen. Informationele privacy is daarbij het recht van een individu op een zorgvuldige informatieverwerking van zijn of haar persoonsgegevens.

De regelgeving voor die informatieverwerking is gestoeld op een aantal door de OESO en de Raad van Europa geformuleerde privacy principes. Dit betreft het principe dat helder is waarvoor de data verzameld wordt, de gegevensverzameling beperkt blijft tot hetgeen nodig is, dat het gebruik van de data beperkt blijft tot het doel waarvoor de data verzameld is, dat de persoonsgegevens juist en nauwkeurig zijn en dat de persoonsgegevens adequaat beveiligd worden. Voorts heeft iedere persoon van wie persoonsgegevens worden verwerkt een individueel recht op transparantie (informatie), het recht op inzage, het recht op correctie, soms het recht om bezwaar te maken (verzet), soms het recht op toestemming voor het gebruik van de gegevens, soms het recht op verwijdering van zijn of haar gegevens, een klachtrecht en een recht op schadevergoeding. Tevens dient de organisatie zich te kunnen verantwoorden voor het gebruik van persoonsgegevens.

Europa wordt gezien als één digitale ruimte met vrij gegevensverkeer en de Nederlandse Wet Bescherming Persoonsgegevens (WBP) heeft daarom zijn basis in een Europese Richtlijn. Gezien de toenemende digitalisering en mogelijkheden tot koppelingen en uitwisseling van gegevens, incidenten waarbij persoonsgegevens op straat komen te liggen en incidenten van oneigenlijk gebruik van persoonsgegevens wordt momenteel door de wetgever gewerkt aan verscherping van de regelgeving. Naar verwachting wordt in 2015 in Nederland de meldplicht datalekken ingevoerd, met boetemogelijkheden tot waarschijnlijk € 450.000 voor het niet-naleven van de meldplicht. Ook zal het College Bescherming Persoonsgegevens in 2015 waarschijnlijk boetebevoegdheden krijgen op handhaving van de WBP, waarbij bedragen van € 810.000 per incident worden genoemd. Tenslotte wordt waarschijnlijk komend jaar een nieuwe Europese privacy verordening aangenomen met boetemogelijkheden tot mogelijk 5% van de jaaromzet van bedrijven of € 100.000.000 voor bedrijven en overheidsinstellingen die onbehoorlijk omgaan met persoonsgegevens. De Europese privacy verordening zal dan waarschijnlijk vanaf 2017 de Nederlandse WPB vervangen. Inhoudelijk volgt de Europese privacy verordening de OESO privacy principes, maar met een zwaarder accent op externe verantwoording (accountability). Die aanscherping zal leiden tot een groot aantal verplicht te nemen beheersmaatregelen ter bescherming van de persoonsgegevens. Dataverwerking en privacybescherming worden daarmee een onderwerp van de bestuurstafel.

Met de opkomst van boetes kan een instelling bij een onbehoorlijke omgang met persoonsgegevens ook eerder en grotere schadeclaims verwachten van benadeelden. Daarnaast zal een incident reputatieschade veroorzaken.
Met de opkomst van boetes is er sprake van een materieel risico voor een instelling bij niet naleving van de (toekomstige) Europese privacy verordening- en –wetgeving. Daardoor zullen ook jaarrekeningaccountants vragen naar bewijzen dat de leiding ‘in control’ is. Dat kan bijvoorbeeld door middel van een managementsysteem aanpak op privacy. Als de accountant meent dat de bedrijfsleiding niet in control is, zal zij eisen dat er substantiële voorzieningen voor toekomstige boetes worden getroffen.

Met een gepast beleid voor privacy compliance kan een instelling een balans realiseren voor de verschillende belangen, persoonlijke risico’s en praktische beheersmaatregelen en hierover verantwoording afleggen. Binnen SURF is een ontwikkeling gaande om instellingen zich tijdig te laten voorbereiden op de komende wijzigingen van de Europese regelgeving.

8.8 Kennisveiligheid

Een instelling voor Hoger Onderwijs is een kennisfabriek waar waardevolle kennis wordt gecreëerd en beheerd. Kenniscreatie of onderzoek wordt doorgaans met andere partijen gedaan, met andere kennisinstellingen of met commerciële partijen. Ook wordt onderzoek uitgevoerd voor derde partijen. In het kader van het hoofdlijnenakkoord hebben instellingen tevens afspraken gemaakt over kennisvalorisatie, kort gezegd hoe de ontwikkelde ‘kennis’ in het hoger onderwijs vermarkt kan worden (“van kennis naar kassa”). Daartoe werken universiteiten en hogescholen als kennisinstellingen samen met bedrijven en overheden in publiek-private partnerships. Als deze kennis ongewild in verkeerde handen beland lopen instellingen grote schade. Naast het beschermen van intellectueel eigendomsrecht is het oog houden voor kennisveiligheid wezenlijk. Er staan immers grote belangen op het spel.
Soms wordt kostbare kennis van derden aan een instelling voor Hoger Onderwijs toevertrouwd.
De instelling kan dus belast zijn met het beschermen van kostbare kennis. Kennisname door onbevoegden, per abuis of opzettelijk – ook wel spionage genoemd – en verlies van die kennis kan ernstige gevolgen hebben voor de reputatie.

Zo komt het voor dat tekortschietende kennisveiligheid derden in de gelegenheid stelt kennis te patenteren die in de instelling is ontwikkeld. Rechtszaken over schending van intellectueel eigendom kunnen daar weer een vervolg op zijn. Een ander risico is dat kennis die door de instelling is ontwikkeld, wordt ontvreemd en misbruikt. Nucleaire proliferatie door Pakistan is daar een voorbeeld van. Soms overtreedt een instelling te goeder trouw de Nederlandse export regelgeving in het kader van het Non-proliferatieverdrag. Ook dat is een vorm van 'kennisveiligheid', evenals imagoschade door incidenten van bedrijfsspionage en schadeclaims van contractpartners bij tekort schietende kennisveiligheid.

Het verbeteren en borgen van kennisveiligheid is vooral een kwestie van bewustwording en alertheid van onderzoekers, medewerkers en studenten. Een gedragscode die richting geeft over hoe om te gaan met kennisuitwisseling, bijvoorbeeld op congressen, in samenwerkingsprojecten en in publicaties is een goede basis voor een betere kennisveiligheid. Ook kan een instelling denken aan zaken als concurrentiebeding, screening van personeel en geheimhoudingsverklaringen. Het rubriceren, afschermen en pattenteren van informatie zijn maatregelen die ook de kennisveiligheid bevorderen.

8.9 Internationalisering

Studenten, onderzoekers en medewerkers van een instelling voor Hoger Onderwijs reizen steeds vaker en langer naar bestemmingen in het buitenland. De één is gepokt en gemazeld en loopt niet in zeven sloten tegelijk. Anderen zijn nog niet eerder ver van huis geweest of komen voor het eerst met een vreemde cultuur in aanraking.
Zijn deze personen wel goed voorbereid op mogelijk vreemde en mogelijk risicovolle omstandigheden? Is er een procedure beschikbaar en zijn verwijzingen naar relevante documentatie actueel om je op de reis voor te bereiden of die een kader bieden om juist niet af te reizen? Is iemand aangesteld om de veiligheid van de reizende studenten of medewerkers te monitoren en om bij calamiteiten in te springen? Wordt voldoende rekening gehouden met cultuur verschillen en afwijkende gewoontes en regelgeving? Zijn de medische voorzieningen en primaire levensomstandigheden in kaart gebracht en is de reizende daarop voorbereid?
In andere landen kunnen afwijkende normen en regels gelden voor bijvoorbeeld het nuttigen van alcohol- en drugs, de do's en don'ts van het nachtleven en de seksuele moraal. Taboes en omgangsvormen zijn soms vreemd en onverwacht.
Een goede reisvoorbereiding zal ook aandacht schenken aan risico's van beroving, verlies van paspoort, ongevallen en ernstige ziekte. Het plotseling moeten terugkeren wegens familieomstandigheden kan aandacht behoeven. Ook zou de instelling moeten zijn voorbereid op de vermissing van een medewerker of student in het buitenland.

Studenten, onderzoekers en medewerkers van buitenlandse Instellingen voor Hoger Onderwijs komen ook steeds vaker naar Nederland. De instelling is dan mogelijk de gastheer en enige toeverlaat voor deze reizigers. Heeft de instelling hen voldoende geïnformeerd over de situatie in Nederland, de vestigingsplaats en instelling? Zijn die mensen door de eigen organisatie goed op hun reis en verblijf in Nederland voorbereid? In welke mate zijn deze mensen zelfredzaam?

Het is te overwegen iemand aan te wijzen als vraagbaak en vertrouwenspersoon voor reizigers. Een handreiking voor reizigers met informatie over afwijkende normen en regels in het buitenland, suggesties voor een goede reisvoorbereiding en vindplaats voor nadere informatie over relevante reisbestemmingen zal vaak van pas komen. Een brochure in de Engelse taal voor bezoekende studenten en onderzoekers is aan te raden als de instelling deze wil aantrekken.

Tot slot moet met internationale uitwisseling ook rekening worden gehouden met de risico's vanuit kennisveiligheid. Denk daarbij aan het gebruik van tablet, laptop en telefoon in het buitenland en andere digitaal opgeslagen informatie zoals contactgegevens en inloggegevens.

Het deelproject Internationalisering heeft tools beschikbaar gemaakt voor bewustwording op veiligheidsrisico's rondom internationalisering.

8.10 Gebouwveiligheid

Bij een instelling voor Hoger Onderwijs komen veel mensen in gebouwen samen. Het waarborgen van de veiligheid van die mensen is één van de belangrijkste verantwoordelijkheden van de instelling. Al het mogelijke moet gedaan worden om een incident met menselijk letsel te vermijden. Ook moeten maatregelen zijn getroffen om na een incident de slachtoffers en aanwezigen zo snel en gecontroleerd mogelijk in veiligheid te brengen.

De regels voor het oprichten en gebruiken van gebouwen zijn vastgelegd in de Woningwet. De Woningwet stelt in het artikel 1a de eigenaar van een gebouw als primair verantwoordelijke voor de veiligheid. In de tweede plaats is de verantwoordelijkheid bij de gebruiker, voor zo ver dat in diens vermogen ligt. De Woningweet 'stuurt' het Bouwbesluit 2012 aan, waarin de bouwregels praktisch zijn vastgelegd. Het Bouwbesluit geeft de minimale eisen aan; het niet voldoen aan deze eisen betekent dat een gebouw niet voldoet aan het wettelijk minimum.

Dit betekent dat bij veiligheidsincidenten eerst de eigenaar en/of de gebruiker worden aangesproken. Bij incidenten kan achteraf worden gekeken of aan de eisen werd voldaan. Met andere woorden, de afgifte van een vergunning of het bekende 'controlerondje' door de brandweer zijn geen garantie dat aan de eisen wordt voldaan.

In het Bouwbesluit zijn eisen opgenomen betreffende de veiligheid, de gezondheid, de bruikbaarheid, de energiezuinigheid en het milieu, de installaties en het gebruik. Deze eisen zijn echter NIET gericht op de continuïteit van de organisatie na een calamiteit. Hiervoor dient de eigenaar of de gebruiker de eigen risico's in te schatten en waar gewenst aanvullende maatregelen te treffen. Ook de mogelijke eisen van een verzekeraar gaan doorgaans boven de eisen vanuit het Bouwbesluit. Ook stelt het Bouwbesluit geen eisen aan bijvoorbeeld de BHV organisatie in een gebouw.
De Omgevingsvergunning bundelt de verschillende vergunningen van een locatie, waaronder de vergunningen die voortvloeien uit het Bouwbesluit.

Naast mensen zijn er natuurlijk ook andere belangen die fysieke bescherming nodig hebben om de continuïteit van de instelling te waarborgen of om andere schade te beperken. Denk aan belangrijke bedrijfsprocessen, ICT en andere bijzondere bedrijfsmiddelen en het gebouw zelf. De eisen vanuit Bouwbesluit en Omgevingsvergunning zijn op safety gericht en NIET op de continuïteit van de organisatie. De instelling moet een eigen visie hebben op het brandveiligheidsniveau van de datacenters en andere essentiële voorzieningen. Dit geldt ook voor bescherming tegen water, kou en hitte. De maatregelen moeten op verschillende bedrijfssituaties worden afgestemd. Een gebouw in nachtsituatie is anders dan in normale gebruikssituatie of tijdens een bijzonder evenement.

De gebouwveiligheid moet rekening houden met criminaliteit, waaronder inbraak, diefstal en vernieling, maar ook met hinder en overlast. Met aanpakken als CPTED (crime prevention through environmental design) kan kosteneffectief een omgeving gecreëerd worden waar gebruikers zich sociaal veilig voelen. Ook zal de gebouwveiligheid rekening moeten houden met brand, blootstelling aan gifgassen en rook, explosies, verstoringen van openbare orde waardoor paniek ontstaat, natuurgeweld en verkeersongevallen op of in de omgeving van de locatie.

Op het gebied van beveiliging tegen diverse vormen van moedwillig handelen en sociale veiligheid zijn er weinig wettelijke eisen. Een uitzondering zijn de gebouwen met de woonfunctie (studentenwoningen), waar in geval van nieuwbouw wel enige concrete eisen zijn gesteld vanuit het Bouwbesluit 2012. Het is aan het bestuur van de instelling om keuzes te maken welke belangen beschermd moeten worden tegen wat voor dreigingen en op welk niveau.

8.11 Crisismanagement, BHV, BCM

Iedere zichzelf respecterende organisatie van enige omvang is op een crisis voorbereid. In deze leidraad zijn de veiligheidsterreinen waarop een crisis kan ontstaan al de revue gepasseerd. Op al die terreinen kan de instelling preventieve maatregelen hebben getroffen. En natuurlijk hoopt iedereen dat die maatregelen afdoende zullen zijn om een mogelijke crisis tijdig af te wentelen. Ook de instelling kan met een crisissituatie worden geconfronteerd. Is deze daar voldoende op voorbereid? Zijn taken en verantwoordelijkheden al toebedeeld? Weet een ieder wat er van hem of haar wordt verwacht? Zijn adequate hulpmiddelen voor handen? Is men geïnformeerd, geoefend en bekwaam?

Voorbereiden op een adequate crisisbeheersing is vooral een kwestie van doen. Het toebedelen van taken, middelen en verantwoordelijkheden en bijvoorbeeld het informeren en oefenen van medewerkers verdient voortdurende aandacht van het management. Oefenplannen en –cycli kunnen daarbij helpen. Naast het informeren en oefenen van medewerkers en studenten kunnen specifieke oefeningen worden georganiseerd voor bijvoorbeeld het bestuur, het management, de IT-afdeling of BHV'ers. Ook kunnen integrale oefeningen met een bepaald thema worden georganiseerd zoals 'studenten vermist in het buitenland' of 'grote brand in het hoofdgebouw'.

Tot het crisismanagement behoort ook het BHV-domein (bedrijfshulpverlening) dat zich richt op het in veiligheid brengen van mensen tijdens een incident. Met een bedrijfscontinuïteit aanpak kan de instelling ervoor zorgen dat na een incident de belangrijkste processen tot op een bepaald niveau kunnen blijven functioneren. Zo vindt het herstel van de situatie in een geaccepteerde tijdsperiode plaats. Tot slot is een geoefende crisiscommunicatie van belang om belanghebbenden tijdens de crisis van de goede informatie te voorzien om daarmee vervolgschade en reputatieschade te beperken.

Check

De check-fase van de managementcyclus evalueert de werking.

9 Evaluatie van de werking

Conform de managementstructuur zal de Instelling voor Hoger Onderwijs haar veiligheidsplannen, -procedures en getroffen veiligheidsmaatregelen bij voortduring monitoren en evalueren. Hiertoe wordt een cyclus doorlopen van periodieke management reviews, onderzoeken, testen, oefeningen en audits.

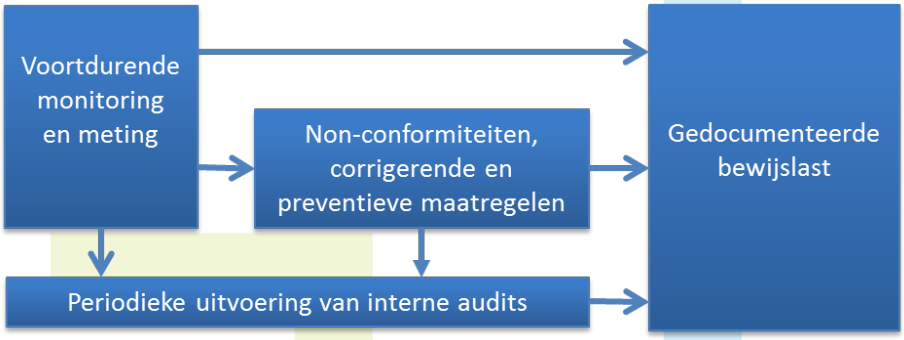
Alle voorkomende veiligheidsincidenten worden onderzocht en geëvalueerd.

De instelling houdt een overzicht bij van uitgevoerde onderzoeken en de daaruit getrokken conclusies en aanbevelingen.

Behalve incidenten dienen scenario's geëvalueerd te worden. Wat is de kwetsbaarheid (mogelijkheid) van dit scenario en wat is de response van de organisatie als dit scenario zich voor zal doen? Is dit acceptabel voor het bestuur en belanghebbenden?

Het is ook mogelijk om het verbetertraject op MIVH te starten in de check-fase. Er wordt dan gestart met een scan van de huidige situatie. Uit de resultaten van die scan worden probleemgebieden gesignaleerd om als eerste aan te pakken. Dit is dan input voor een managementbeslissing (fase management review) op de start en doelstelling van een verbetertraject.

Het zich kunnen verantwoorden op de veiligheidsprestatie is essentieel voor een instelling en tussen de activiteiten in de check- en de act-fase zijn de volgende relaties:



Een basisprincipe is dat de veiligheid en de veiligheidprestaties meetbaar worden gemaakt. Hierbij kunnen bijvoorbeeld KPI's worden gedefineerd of andere doelstellingen en afgeleide kenmerken die meetbaar zijn. Hier wordt in 9.1, maar ook in 8.1 op ingegaan.

Op die kenmerken zijn voortdurende activiteiten op monitoring en meting. Denk aan testen, oefenen en dagrapportages. De resultaten worden als bewijslast bewaard om aantoonbaar te maken dat de veiligheidsprestatie functioneert.

Indien uit de meting blijkt dat de veiligheidsprestatie op een onderdeel niet functioneert, dan worden daar corrigerende en preventieve maatregelen op uitgevoerd. Zie hiervoor 10.1. De resultaten worden als bewijslast bewaard.

Periodiek worden interne audits uitgevoerd. Zie hiervoor 9.2. Input voor de interne audit zijn onder meer de resultaten uit de voorturende monitoring en meting, maar ook wat de non-conformiteiten waren die gecorrigeerd zijn. Ook de resultaten van de interne audit worden vastgelegd als bewijslast.

9.1 Bewaking, meting, analyse en evaluatie

Een veel beproefd instrument om te monitoren is het uitvoeren van een zelfbeoordeling. De operationeel en de beleidsmatig verantwoordelijken van een proces of veiligheidsthema krijgen via deze zelfbeoordeling inzicht in de kwaliteit van dat veiligheidsproces en kunnen op basis daarvan bijsturen.

De bewaking en meting van de veiligheidsprestatie kan volgens de boekjes het beste op KPI's (kritieke prestatie indicatoren) worden gedaan. De instelling zal deze dan voor alle veiligheidsthema's opstellen. Maandelijks, per kwartaal en jaarlijks worden selecties van deze KPI's in een management rapportage samengevat en toegelicht. Trends en mate van volwassenheid per veiligheidsthema worden hiermee inzichtelijk gemaakt.

In de praktijk blijkt het vaak lastig om goede KPI's te definiëren. Mogelijk is het zinvol om vanuit de community of practice de nuttige KPI's te vinden. Daarbij zijn er verschillende bronnen. Inventariseer welke KPI's al in de verschillende domeinen worden gebruikt. Diverse KPI's zijn nodig in de externe verantwoording en liggen min of meer vast. Daarnaast zijn er instelling specifieke indicatoren waarmee actief gestuurd kan worden op verbetering van de veiligheid (act).

Uit deze inventarisatie kan een stelsel van KPI's worden opgesteld als bijvoorbeeld 'gemiddeld aantal incidenten per medewerker (de medewerker gaat in de fout)'; 'gemiddeld aantal incidenten per buitenlandse student (student is slachtoffer)'; 'aantal FTE's belast met veiligheidstaken'.

Een instelling zal regelmatig oefeningen en testen organiseren om de werking en effectiviteit van getroffen veiligheidsmaatregelen te evalueren. Verschillende veiligheidsthema's kunnen gelijktijdig (integraal) hierin worden betrokken. Oefeningen en testen (O&T) zullen worden georganiseerd, rekening houdend met:

- doelstellingen, verantwoordelijkheden en taak van de instelling;
- doel, omvang en impact van de O&T;
- risico's die O&T met zich meebrengt;
- resultaten van voorgaande O&T.

Een belangrijke bron is de incidentregistratie. Voor alle betrokkenen moet het helder zijn waar incidenten gemeld kunnen worden. Vanuit dit meldpunt moet de melding naar een interne of externe partij worden gebracht voor verdere beoordeling en behandeling. Denk bijvoorbeeld aan een onderscheid tussen ICT-incidenten, fysieke beveiligingsincidenten en incidenten rondom personen. Uit de incidentregistratie komt managementinformatie op type incidenten, type kwetsbaarheden en de effectiviteit van het behandelproces op deze incidenten. Vanuit deze informatie kunnen verbeterplannen worden opgesteld.

9.2 Interne audits

Voor de positionering van de interne audit is het nuttig om het volgende onderscheid te maken:

- Een zelfbeoordeling wordt uitgevoerd door degene die het object is van de beoordeling (slager keurt eigen vlees) en dient vooral als voorbereiding op een interne of externe audit.
- Een interne audit wordt uitgevoerd voor de eigen organisatie en kan door eigen medewerkers maar ook door externen worden uitgevoerd. De resultaten worden vooral gebruikt voor de verbetering van de eigen organisatie.
- Een externe audit wordt uitgevoerd om de buitenwereld te laten zien wat het niveau is van het veiligheidssysteem. De externe audit wordt geleid vanuit een externe partij.

Een instelling zal jaarlijks interne audits organiseren per veiligheidsthema of daar waar mogelijk voor verschillende thema's samen. De instelling zal een auditprogramma vaststellen, implementeren en onderhouden, met inbegrip van methoden, verantwoordelijkheden en rapportage. Een auditprogramma zal het belang van de desbetreffende processen en de uitkomsten van voorgaande audits hierin betrekken.
Aandacht zal onder andere worden besteed aan:

- eisen die de instelling heeft gesteld zoals in de reikwijdte vastgesteld (zie 4.3);
- doelstellingen, processen en procedures voor veiligheid;
- efficiëntie en doelmatigheid van maatregelen;
- resultaten van eerdere oefeningen, testen en reviews.

Naast interne audits zijn er ook diverse externe audits. Veiligheidsmaatregelen rondom contractonderzoek kunnen extern worden beoordeeld, maar ook laboratoria zullen regelmatig extern getoetst worden op het behoud van de vergunning. Deze toets zal in de regel geïnitieerd worden door de vergunningverlener en zal worden uitgevoerd door de eigen organisatie, een bevoegde externe specialist en mogelijk ook gebruik maken van interne toetsingsresultaten van de instelling.
Maak een overzicht van de externe audits die uitgevoerd moeten worden en onderzoek mogelijkheden om de uitvoering van die audits te vereenvoudigen, waardoor sneller een positief resultaat verkregen wordt met een kleinere belasting voor de eigen organisatie.

9.3 Management review

De instelling onderzoekt jaarlijks in welke mate de veiligheidsthema's integraal worden beheerd en of er voortdurend aan verbetering wordt gewerkt. De effectiviteit van het MIVH wordt beoordeeld. Het onderzoek is gebaseerd op:

- voorgaande onderzoeken en reviews met conclusies en aanbevelingen;
- voortgang van de implementatie van eerdere aanbevelingen;
- adviezen en aanbevelingen van (externe) veiligheidsexperts;
- resultaten van audits, oefeningen en testen;
- ontwikkelingen in de gerapporteerde KPI's;
- in- en externe ontwikkelingen.

De jaarlijkse management review biedt conclusies en aanbevelingen ten aanzien van:

- integraal managen van veiligheid;
- effectiviteit van gevoerd beleid (getroffen maatregelen);

- actualisering van dreigings-, impact- en risicoanalyses;
- paraatheid en geoefendheid van de crisisorganisatie;
- actualiteit van crisisplannen;
- verbeteringen van veiligheidsplannen, -procedures en –maatregelen;
- allocatie van middelen voor alle veiligheidsthema's.

In de organisatie (zie 5.3) wordt vastgelegd wie de betrokkenen zijn van de managementreview. Naast bestuur kunnen dat ook proceseigenaren zijn. De bestuurder of manager die de managementreview ondertekent geeft daarbij aan dat deze op de hoogte is van alle relevante onderzoeken, daaraan zelf conclusies in relatie tot het MIVH heeft verbonden en welke activiteiten de komende tijd zullen worden uitgevoerd en dat daar ook voldoende mankracht en middelen beschikbaar voor zijn.

9.4 Evaluatie per veiligheidsthema

Toetsingsinstrumenten
Enkele veiligheidsthema's van het MIVH beschikken over een eigen evaluatie instrumentarium waar een instelling gebruik van kan maken. Hieronder is een overzicht van instrumenten die beschikbaar zijn. Daarnaast bestaan ook diverse toetsingsinstrumenten van commerciële partijen op verschillende thema's.

Wat betreft gebruik van deze instrumenten is het 'Comply or explain'. Gebruik de toetsingsinstrumenten. Er kunnen redenen zijn om deze instrumenten niet te gebruiken, maar geef dan uitleg hoe dan wel tot een gepast veiligheidsniveau wordt gekomen.

	Governance, risk, compliance	Arbeidsomstandigheden	Milieuveiligheid	Sociale veiligheid	Integriteit	Informatieveiligheid	Privacy	Kennisveiligheid	Internationalisering	Gebouwveiligheid	Crisismanagement, BHV, BCM
SURF, Normenkader , assessments en benchmark. Dit betreft een normenkader gebaseerd op ISO27002 op informatiebeveiliging, continuïteit van bedrijfsgegevens en privacy.						x	x				
Integrale Veiligheid Hoger Onderwijs, SAINT (self assessment integriteit).					x	x		x			

Toetsing op regulering

De regulering bestaat uit het wettelijke kader en de zelfregulering van de branche. Een toets op het voldoen aan deze regulering kan alleen plaatsvinden na het expliciet maken van het juridisch kader per proces.

Start hierbij om de processen te identificeren en de typologie hiervan vast te stellen. Vanuit die typologie kunnen de wettelijke- en zelfreguleringseisen worden geïdentificeerd. Locaties/processen met een eigen typologie aan regelgeving zijn bijvoorbeeld de catering/keuken, laboratoria, helikopter landingsplaats, parkeergarage of grote evenementen. Vaak is slechts een deel van de regelgeving relevant voor een locatie of een proces. Dit leidt tot een tabel waarbij per proces/locatie helder wordt gemaakt op welke onderdelen van regelgeving getoetst zal worden en verantwoording op zal worden afgelegd. Ook kan worden vastgelegd op welke onderdelen van de wet- en regelgeving niet direct hoeft te worden getoetst. Het beschikken over een document waarop heldere keuzes staan op relevante reguleringseisen en eisen die minder relevant worden gevonden, is op zich zelf al een belangrijk verantwoordingsmiddel.

Onderstaande tabel geeft een eerste aanzet op veel voorkomende regelging en de veiligheidsthema's waarop deze van toepassing is. Vanuit de community of practice zou een verdere detaillering gemaakt kunnen worden naar processen.

	Governance, risk , compliance	Arbeidsomstandigheden	Milieuveiligheid	Sociale veiligheid	Integriteit	Informatieveiligheid	Privacy	Kennisveiligheid	Internationalisering	Gebouwveiligheid	Crisismanagement, BHV, BCM
Aanbestedingswet					x						
Arbeidsomstandighedenwet, met Arbeidsomstandighedenbesluit en NEN normen		x								x	x
Asbestwet			x								
Burgerlijk wetboek (o.m. onrechtmatige daad)		x	x	x	x	x	x	x	x	x	x
Drank en horecawet										x	
Kernenergie wet			x							x	
Luchtvaartwet (helikopter landingsplaats)										x	
Tabakswet (rookvrije ruimten)		x								x	
Warenwet (behandeling levensmiddelen)			x							x	
Waterwet (drinkwater, lozing afvalwater)			x								
Wet Bescherming Persoonsgegevens							x				
Wet Computercriminaliteit						x					
Wet op dierproeven			x							x	
Wet op hoger onderwijs & wetenschappelijk onderzoek	x			x							
Wet op de particuliere beveiligingsorganisaties en recherchebureaus					x					x	
Wet voorkoming misbruik chemicaliën			x							x	
Wet milieubeheer (bodemkwaliteit)			x								
Woningwet, met Bouwbesluit en Omgevingsvergunning. Zie ook opmerking bij Bijlage 1 – 9 Gebouwveiligheid .			x							x	x
Wet ter voorkoming van witwassen en financiering					x			x			

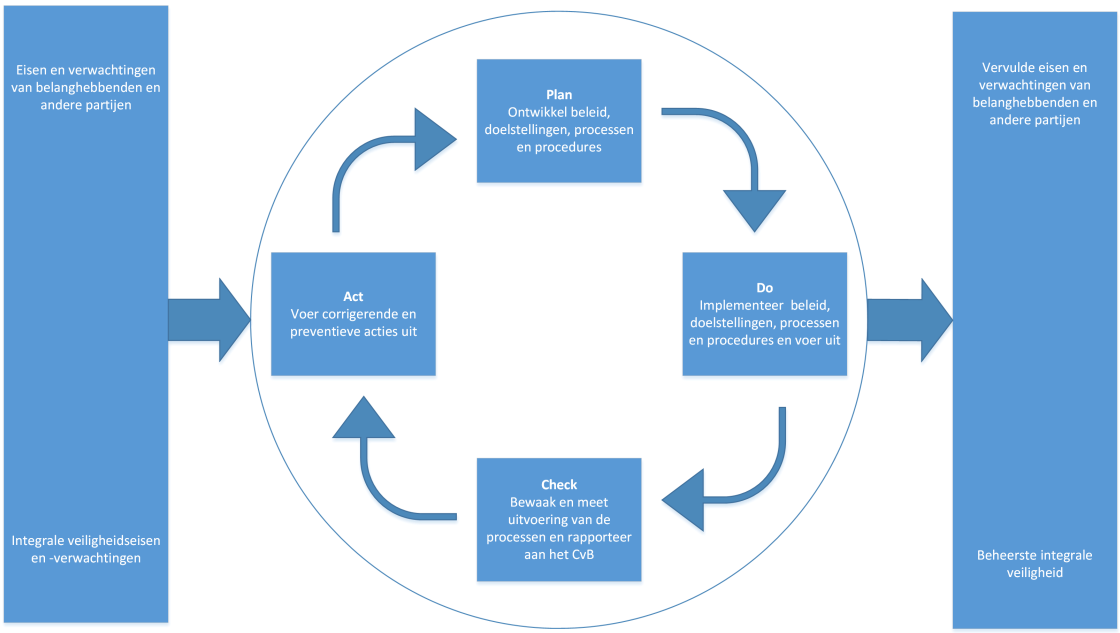
	Governance, risk , compliance	Arbeidsomstandigheden	Milieuveiligheid	Sociale veiligheid	Integriteit	Informatieveiligheid	Privacy	Kennisveiligheid	Internationalisering	Gebouwveiligheid	Crisismanagement, BHV, BCM
van terrorisme											
Wetboek van Strafrecht		x	x	x	x	x	x	x	x	x	
Wetboek van Strafvordering		x	x	x	x	x	x	x	x	x	
Regeling Jaarverslaggeving Onderwijs (RJO) is wettelijk kader op verslaglegging. RJO is gebaseerd op de Ontwerp Richtlijn 400 Jaarverslag van de Raad voor de Jaarverslaglegging. Als verbijzondering van RJO stelt de Inspectie voor Onderwijs het zg Onderwijsprotocol op. Deze instructie geeft aan waarop gerapporteerd moet worden. Onderwijsprotocol eist paragraaf op continuïteit, milieuveiligheid, sociale veiligheid en privacy.			x	x			x				x
Uitvoeringsregeling stralingsbescherming			x							x	
Klokkenluidersregeling					x						
Integriteitscode of gedragscode											
Regeling ongewenst gedrag				x							

Act

In de act-fase van de managementcyclus wordt de verbetering op de veiligheid opgestart.

10 Verbetering

In de act-fase van de managementcyclus worden de correcties en verbeteracties voor de veiligheidsthema's en het managementsysteem geïnitialiseerd. Vanuit eerder verkregen stuurinformatie worden deze acties opgesteld.



10.1 Non-conformiteiten en corrigerende acties

Een instelling kan veel winst halen uit een goede non-conformiteiten procedure.

Informatiebronnen die non-conformiteiten aan het licht kunnen brengen zijn onder meer self asessments, incident rapportages, inspectie- en onderhoud rapporten, project rapportages, audit rapportages, informatie met betrekking tot situaties en gebeurtenissen met bijzondere risico's, klachten en verontrustingen van belanghebbenden en non-compliance constateringen op regelgeving. Per veiligheidsthema kan het melden en verzamelen van non-conformiteiten ingericht worden.

Na het constateren van een non-conformiteit zijn verschillende acties mogelijk. De non-conformiteit moet aangepakt worden en als er schade is zullen ook de gevolgen moeten worden afgehandeld. Daarnaast kan gekeken worden naar de oorzaken van de conformiteit. Zijn er maatregelen te treffen op de oorzaak van de conformiteit, waardoor de kans op herhaling verkleind wordt? Staat de non-conformiteit op zichzelf of kunnen er meerdere vergelijkbare situaties zijn? In de laatste situatie moet actief gezocht worden naar vergelijkbare non-conformiteiten om die aan te pakken. Door een actieve opstelling leidt iedere geconstateerde non-conformiteit tot een verbetering van de veiligheidsaanpak.

De resultaten moeten als bewijslast worden bewaard, waardoor verantwoording op de veiligheidsprestatie van de instelling mogelijk wordt.

Vanwege het aantal veiligheidsthema's en de mogelijk grote hoeveelheid corrigerende acties die gemanaged moeten worden, is het aan te raden hiertoe een register of systeem aan te leggen. De instelling zal daarin onder andere bijhouden van alle veiligheidsthema's de non-conformiteiten, hoe daarmee om te gaan en de actuele stand van zaken. In dat register kan ook worden bijgehouden, of worden verwezen naar documenten waarin is opgenomen de analyse van de tekortkomingen met onder andere de oorzaak of oorzaken van de tekortkoming, de ernst daarvan (mogelijk verhoogd risico), mogelijke schade beperkende maatregelen, de kosten daarvan, de effectiviteit van die maatregelen, een kosten-baten analyse, een analyse of vergelijkbare tekortkomingen kunnen ontstaan.

10.2 Voortdurende verbetering

Een instelling voor Hoger Onderwijs vertaalt de conclusies en aanbevelingen van management reviews, oefeningen, testen en audits in verbeteringen van het integrale veiligheidsmanagement systeem en naar concrete veiligheidsmaatregelen.
Daar waar niet aan geldende wetten en normen wordt voldaan, worden deze 'Non-conformiteiten' binnen afzienbare termijn weggenomen. De verbeteringen moeten het ontstaan van nieuwe 'non-conformiteiten' in de toekomst vermijden.

Het bestuur en management zal deze verbeteringen uitdragen, op de uitvoering daarvan toezien en hierover in het Jaarverslag rapporteren. Jaarlijks dient voldoende budget voor het beheren en verbeteren van het MIVH te worden toegewezen.

Bij verbeteringen van het MIVH zal telkens bezien moeten worden in welke fase van de veiligheidsketen de investeringen het best tot hun recht komen. De prioritering van verbeteringen vindt mede plaats op basis van de mate dat de verbetering bijdraagt aan de beoogde risicoreductie.

Dreigingsbeelden, impact- en risicoanalyses, stresstests en onderzoeken naar kwetsbaarheden dienen geactualiseerd of periodiek herhaald te worden. Mogelijk dat deze analyses aanleiding zullen zijn om maatregelen bij te stellen. Maar ook als geen bijstellingen van maatregelen nodig zijn, zijn deze analyses onderdeel van de voortdurende verbeteringen van het MIVH.

Verbeteringen worden SMART geformuleerd en eenduidig belegd binnen de organisatie. Voorgenomen verbeter acties, de planning van de activiteiten, de afronding en oplevering zullen worden gedocumenteerd. Geïmplementeerde verbeteringen worden op effectiviteit geëvalueerd.

Het MIVH zal planmatig en gedocumenteerd worden onderhouden en doorlopend worden verbeterd
De instelling verbetert en actualiseert de documentatie van het MIVH continue. In een procedure zullen de volgende aspecten van de MIVH documentatie worden geregeld: actualisering, beveiliging, toegang, verspreiding, opslag, bewaartermijn en vernietiging.

Bijlage 1: Bronnen

Een instelling voor Hoger Onderwijs dient te voldoen aan de Nederlandse wet- en regelgeving. Bovendien zijn een aantal normen van toepassing op deze instelling. In deze bijlage zijn normen en good practices voor de hoger onderwijs instellingen geïnventariseerd en aangehaald bij de verschillende veiligheidsthema's.

0 Algemeen, Governance, Risk, Compliance

Organisatie

- Projectgroep Integrale Veiligheid Hoger Onderwijs, 2012, Integrale veiligheid in governance en bedrijfsvoering in het hoger onderwijs is de handleiding voor de implementatie van integrale veiligheid in hoger onderwijs.
- ASIS International (ANSI/ASIS SPC.4-2012), Maturity Model for the Phased Implementation of the Organizational Resilience Management System is een handleiding op gefaseerde implementatie en normenkader met zes volwassenheidsniveaus op de NEN 7131. Deze NEN 7131 (organizational resilience management system) is een referentie managementsysteem van de MIVH.
- Julian Talbot & Miles Jakeman (2009), Security Management Body of Knowledge, geeft een helder inzicht op de hedendaagse opvattingen op security management.

Functiebeschrijvingen

- SURF, Leidraad Functieprofiel Informatiebeveiliger geeft functieomschrijvingen voor de meest voorkomende informatiebeveiligingsfuncties.
- ASIS International, ANSI/ASIS CSO.1-2013, Chief Security Officer – an organizational model geeft profielbeschrijving van security manager.

Overlegorganen

- VSNU: Overleg beveiligingsfunctionarissen van universiteiten
- Vereniging Hogescholen: Overleg beveiligingsfunctionarissen van hogescholen
- Nederlandse Federatie van Universitair Medische Centra: Veiligheidscommissie

Risico's

- OCW Beleidsvisie Veiligheid en radicalisering, 2009. Document definieert een viertal vitale OCW belangen (1 het ongestoord functioneren van OCW instellingen als effectieve en efficiënte (onderwijs, cultuur en wetenschap) systemen; 2. Het ongestoord functioneren van mensen actief voor en binnen OCW instellingen en sectoren; 3. Het ongestoord functioneren van OCW infrastructuur; 4. Het ongestoord voortbestaan van een maatschappelijk klimaat waarin groepen mensen goed met elkaar kunnen samenleven binnen de kaders van de democratische rechtstaat en gedeelde kernwaarden) en een achttal dreigingen (CBRN-terrorisme, dierenrechtactivisme, digitale verlamming, overstromingen, pandemieën, CBRN proliferatie, radicalisering, sociale veiligheid).

Bewustwording

- Deelproject Bewustwording van het project Integrale Veiligheid Hoger Onderwijs is gericht op vergroting van de bewustwording en op het ontwikkelen van hulpmiddelen hierbij voor het hoger onderwijs.

1 Arbeidsomstandigheden

Bronnen

- VSNU Arbocatalogus (www.vsnu.nl/arbocatalogus.html)
  Een catalogus opgesteld door de VSNU voor de volgende thema's:
  1. Psychologisch sociale arbeidsbelasting (PSA):
     - Ongewenst gedrag naar medewerkers (Seksuele intimidatie, Agressie en geweld, Pesten, Discriminatie, Stalking),
     - Werkdruk en werkstress bij medewerkers
  2. Klachten van armen, nek en schouders (RSI) bij medewerkers en studenten (KANS)
  3. Gevaarlijke stoffen (GS)
  4. Risico-inventarisatie & Evaluatie (RIE)
  5. Bedrijfshulpverlening (BHV)
  6. Voorlichting, Onderricht en Toezicht (VO&T)
- HBO Arbocatalogus (www.arbocatalogushbo.nl)
  Een catalogus opgesteld door de Vereniging Hogescholen met de volgende thema's:
  1. Gezonde werkplek (Beeldschermwerk, Zittend werk)
  2. Verzuim en preventie
  3. Werkdruk
  4. Ongewenst gedrag (Seksuele intimidatie, Agressie en geweld, Pesten, Discriminatie)
  5. Werk, zwangerschap en borstvoeding
  6. Gevaarlijke stoffen, biologische agentia en machineveiligheid
- Opmerking: De good-practices uit de arbo-catalogi zijn gericht op medewerkers en soms ook op studenten. Dit houdt in dat bepaalde thema's wel voor medewerkers zijn uitgewerkt, maar niet voor studenten.
- College van beroep voor het hoger onderwijs is een onafhankelijke instantie die rechtszaken behandelt op het terrein van hoger onderwijs. Een student kan in beroep gaan als hij het niet eens is met een beslissing van de instelling. Het kan bijvoorbeeld ook gaan op overtreding van huisregels en ordemaatregelen van de instelling.
- NPR 5001 – Model voor een arbo-managementsysteem.
- NTA 8031 – Registratie van arbeids- en bedrijfsongevallen.

2 Milieuveiligheid

Bronnen

- Milieu Effect Rapportage brengt de milieugevolgen van een besluit in beeld voordat het besluit wordt genomen. Zo kan de overheid die het besluit neemt (het bevoegd gezag) de milieugevolgen bij haar afweging betrekken.
- Omgevingsvergunning bundelt alle vergunningen voor het gebruik van een locatie, waaronder de verschillende milieuvergunningen.
- Uitvoeringsregeling stralingsbescherming van het Ministerie van Economische Zaken van oktober 2013. Deze richtlijn geeft beveiligingseisen op weerstand en toegankelijkheid tot radioactieve stoffen.
- Ministerie van Economische Zaken, 2013, Handreiking beveiliging radioactieve stoffen.

- SAAZ-UNIE is de samenwerking van Arbo- en milieudiensten van universiteiten en universitair medische centra. Binnen SAAZ-UNIE bestaat periodiek overleg van de milieu functionarissen, de biologische veiligheidsfunctionarissen en de radiologische/stralingsdeskundigen.

3 Sociale veiligheid

Schoolgeweld

- Centrum School en Veiligheid (www.schoolenveiligheid.nl), Handreiking preventie en omgaan met schoolaanslagen. Ook is er een informatieblad op schietpartijen op scholen.
- M&O Groep in opdracht van NCTV (2013), Handreiking voor signalering en begeleiding veiligheids- en leefstijlrisico's in het HBO.

Ongewenst gedrag

- Centrum School en Veiligheid, diverse handreikingen op ongewenst gedrag: Agressie tegen personeel, Agressieve leerlingen, Agressieve ouders, Discriminatie en racisme, Online pesten, Seksuele intimidatie, Veilige Publieke Taak Onderwijs (dit is een kennisforum op sociale veiligheid bij scholen, www.forumveiligeschool.nl), Wapengeweld

Pedagogisch klimaat

- Centrum School en Veiligheid, diverse handreikingen op pedagogisch klimaat: Burgerschap, Conflictbemiddeling, Gedrag en kleding, Peers, Sociale competenties, Weerbaarheid, Seksuele diversiteit
- Centrum School en Veiligheid, diverse handreikingen op verwante thema's: Huiselijk geweld, Seksueel geweld in de thuissituatie, Eerwraak en huwelijksdwang, Extremisme en radicalisering, Fysieke veiligheid, Veiligheid en handicap, Drugs op school, Mediawijsheid

OPMERKING: School en Veiligheid richt zich op voortgezet onderwijs en MBO. Voor hoger onderwijs dient vertaalslag naar eigen instelling gemaakt te worden.

4 Integriteit

Bronnen

- VSNU (2012), De Nederlandse Gedragscode Wetenschapsbeoefening, principes van goed wetenschappelijk onderwijs en onderzoek.
- Landelijk Orgaan Wetenschappelijke Integriteit (LOWI) is een onafhankelijk adviesorgaan inzake schendingen van wetenschappelijke integriteit.
- Adviescommissie Behoorlijk Bestuur (2013), 'Een lastig gesprek – Advies Commissie Behoorlijk Bestuur'.
- Integrale Veiligheid Hoger Onderwijs, SAINT (self assessment integriteit). Dit betreft een vragenlijst, ontwikkeld door Bureau Integriteitsbevordering Openbare Sector en gebaseerd op de KWAS-analyse (kwetsbaarheidsanalyse spionage) van AIVD op informatieveiligheid, integriteit en kennisveiligheid. Daarnaast is er een group decision applicatie op dit thema. De vragenlijst en de group decesion tool zijn in ontwikkeling.

5 Informatieveiligheid

Informatiebeveiliging

- SURF, SURFibo is het landelijke overleg van informatiebeveiligers in het hoger onderwijs. In SURFibo werkt SURF met hogescholen en universiteiten aan het verbeteren van professionele informatiebeveiliging in het hoger onderwijs. SURFibo heeft een aantal modelteksten beschikbaar.
- SURF, Normenkader , assessments en benchmark. Dit betreft een normenkader gebaseerd op ISO27002 op informatiebeveiliging, continuïteit van bedrijfsgegevens en privacy. Daarbij is ook een assessment beschikbaar, waarbij het helder wordt op welk volwassenheidsniveau van informatiebeveiliging de instelling zich bevindt. Ook is er een benchmarkinstrument.
- NEN-ISO/IEC 27001 – Informatietechnologie – Beveiligingstechnieken – Managementsystemen voor informatiebeveiliging – Eisen.
- NEN-ISO/IEC 27002 – Informatietechnologie – Beveiligingstechnieken – Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging.
- ISO/IEC 27005:2014 Information technology -- Security techniques -- Information security risk management gaat in op risicomanagement met betrekking tot informatiebeveiliging.

Cybersecurity

- Nationaal Cyber Security Centrum (NCSC)
- Integrale Veiligheid Hoger Onderwijs & Surf, Dreigingsbeeld hoger onderwijs. Dit betreft cyber dreigingsbeeld voor hoger onderwijsinstellingen.
- SURF, SURFcert biedt de instelling 24 uur per dag, 7 dagen per week, ondersteuning bij cybersecurity incidenten.

IT bedrijfscontinuïteit management

- SURF, Starterskit Bedrijfscontinuïteit. Dit betreft een aanpak voor het opzetten en onderhouden van continuïteitsplannen voor IT. De starterskit bestaat ook uit een groot aantal voorbeelddocumenten.

Digitale rechten

- SURF, handreikingen op digitale rechten:
  - Auteursrechten
  - Open educational resources (OER)
  - Weblectures
  - Beeld en geluid
  - Learning analytics
  - Licenties
  - Onderzoek data

6 Privacy

Bronnen

- College Bescherming Persoonsgegevens. Diverse uitspraken en richtlijnen, waaronder 'CBP Richtsnoeren Beveiliging van persoonsgegevens'
- SURF, handleidingen, studies en presentaties op privacy:
    - Privacy en cloud
    - Privacy en digitale identiteit
    - Rechtmatig operationeel handelen in ICT
    - Privacy en persoonsgegevens van studenten
    - Diverse seminars ter voorbereiding op nieuwe privacy ontwikkelingen
- VSNU (2005) Gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek
- SURF werkgroep om instellingen in hoger onderwijs te begeleiden op nieuwe regelgeving.

7 Kennisveiligheid

Bronnen

- Integrale Veiligheid Hoger Onderwijs, SAINT (self assessment integriteit). Dit betreft een vragenlijst, ontwikkeld door Bureau Integriteitsbevordering Openbare Sector en gebaseerd op de KWAS-analyse (kwetsbaarheidsanalyse spionage) van AIVD op informatieveiligheid, integriteit en kennisveiligheid. Daarnaast is er een group decision applicatie op dit thema. De vragenlijst en de group decesion tool zijn in ontwikkeling.
- Kwetsbaarheidsanalyse Spionage (KWAS) en Handleiding Kwetsbaarheidsonderzoek Spionage www.aivd.nl/dossiers/spionage
- Brochure 'Spionage in Nederland, wat is het risico?' en brochure 'Spionage bij reizen naar het buitenland, wat is het risico?' en brochure 'Digitale Spionage, wat is het risico?' www.aivd.nl/dossiers/spionage
- NCTV, E-learning Spionage, www.nctv.nl/onderwerpen/spionage
- Toelichtingen spionagerisico's www.aivd.nl/dossiers/spionage/persberichten
- NCSC, Cybersecurity Strategie 2.0 en Cybersecurity Beeld Nederland 3, www.ncsc.nl
- AIVD, Publicatie Bring Your Own Device, www.aivd.nl/dossiers/cyberdreiging/publicaties

8 Internationalisering

Bronnen

- Deelproject Internationalisering (2014) heeft handreiking en bewustwording instrumentarium opgesteld op veiligheidsvraagstukken rond internationalisering.
- Nuffic, Gedragscode Internationale Student in het Nederlandse hoger onderwijs.
- Adviesraad voor Wetenschaps- en Technologiebeleid, Going Dutch (2013). Analyse van de kennissamenleving in internationaal perspectief.

9 Gebouwveiligheid

Algemeen

- Bouwbesluit. De locatie moet aan het bouwbesluit voldoen. Belangrijke eisen uit het bouwbesluit zijn locaties en constructies van de brand- en rookcompartimenteringen en de breedte en uitvoering van de vluchtwegen. Het bouwbesluit is vooral een paraplu waar algemene eisen worden gesteld op verschillende safety-aspecten van het gebouw.
    - In het Bouwbesluit 2012 is bepaald wanneer een brandmeld- en ontruimingsalarminstallatie moet zijn voorzien van een certificaat. Doorgaans is dit bij gebouwen waar sprake is van minder zelfredzame personen en bij grote concentraties van persoenen al dan niet in combinatie met slapen. Voor onderwijs- en kantoorfuncties is er in principe geen eis voor certificatie, tenzij dat deze gebruiksfuncties voorkomen in combinatie met bijeenkomstfuncties. Waar actieve blusinstallaties en rookbeheersing installaties zijn toegepast in het kader van gelijkwaardige veiligheid, is certificatie vereist. De certificatie voorziet in een structurele periodieke controles (met frequenties van 1 of 3 jaar bij wel resp. geen doormelding van brandalarmen naar de brandweer). De brandmeld- en ontruimingsalarminstallatie moeten worden beheerd en onderhouden.
    - Het artikel 1.16 van het Bouwbesluit (Zorgplicht) stelt dat de eigenaar de installaties en de brandwerende scheidingen in een gebouw adequaat moet beheren en onderhouden. De frequentie van controles is echter niet nader bepaald, behalve dat na installatiewerkzaamheden controles op brandwerende doorvoeringen adequaat moeten worden uitgevoerd.
    - De eigenaar kan nadere eisen stellen en eigen systematiek bepalen voor structurele controles.
- Omgevingsvergunning. In de afgifte van de omgevingsvergunning worden maatregelen op de specifieke gebruiks- en safety risico's van het gebouw beoordeeld.

Specifieke NEN normen

- Normen zoals opgenomen in de Regeling Bouwbesluit (laatste versie april 2014)
- Overige normen die bruikbaar zijn voor gebouwveiligheid. Denk bijvoorbeeld aan:
    - NEN-EN-ISO 16000 – Binnenlucht – Deel 1-7: over monsterneming
    - NPR 5313 – Computerruimtes en datacenters – Beveiliging
    - NTA 8012 – Beperking van schade als gevolg van brand van en via de elektrische leidingen in de elektrische installatie
    - NTA 8073 – Vaste brandblusinstallaties – Automatische sprinklerinstallaties
    - NTA 8101 – Termen voor facilitaire voorzieningen toegespitst op het onderwijs – Definiëring en rubricering
    - NPR 1090 – Ventilatie van schoolgebouwen – Voorbeelden van oplossingen voor schoolgebouwen
    - NEN 3140 – Elektrische installaties
- NEN-EN-ISO 20957 – Vast opgestelde trainingsapparatuur – Veiligheidseisen en beproevingsmethoden.
- ISO 55000 – Asset management. In deze norm is ook een risicoanalyse op de assets opgenomen.

Beveiliging en sociale veiligheid

- Centrum voor Criminaliteitspreventie en Veiligheid (CCV), VRKI – Richtlijn inbraakbeveiliging onderwijsinstellingen versie 1.4 maart 2014. Dit betreft richtlijnen op diefstal/inbraak risico.
- Centrum voor Criminaliteitspreventie en Veiligheid (CCV). Veiligheidseffectrapportage (VER). De VER is een procesinstrument om in het ontwikkelingstraject van een locatie met alle veiligheidsaspecten rekening te houden. Het richt zich dan met name op beveiliging, sociale veiligheid en de crisisbestendigheid van de locatie.
- ASIS International, ANSI/ASIS PAP.1-2013, Security Management Standard: Physical Asset Protection is een management systeem aanpak op fysieke beveiliging van locaties.

Evenementenbeveiliging

- NTA 8020 – Evenementenbeveiliging en publieksbeveiligingsdiensten.

10 Crisismanagement, BHV, BCM

Bronnen BHV

- NEN 8112, 'Leidraad voor ontruimingsplannen' en NEN 4000 'Bedrijfshulpverlening' zullen in 2014 worden samengevoegd in een nieuwe NEN 8112 'Bedrijfshulpverlening'. Deze norm zal ook een toolkit bevatten.
- NIBHV 2010, Handleiding BHV 2010, www.nibhv.nl/bhv

Bronnen bedrijfscontinuïteit management

- NEN-ISO 22301:2012-06, Maatschappelijke veiligheid – Managementsystemen voor bedrijfscontinuïteit – Eisen. Dit is het managementsysteem voor bedrijfscontinuïteit management.
- NEN-ISO 22313:2013, Maatschappelijke veiligheid - Business continuity managementsystemen – Leidraad geeft praktische handvatten voor de implementatie daarvan.
- SURF, Starterskit Bedrijfscontinuïteit. Dit betreft een aanpak voor het opzetten en onderhouden van continuïteitsplannen voor IT. De starterskit bestaat ook uit een groot aantal voorbeelddocumenten.

Bijlage 2: Raamwerk voor planning van doelen en acties van het MIVH

De uitvoering van het project is natuurlijk organisatie-specifiek. Houdt het doel in de gaten dat het MIVH in de organisatie geïmplementeerd moet worden. Het MIVH is geen stuk techniek.

Succesfactoren voor de implementatie zijn:

- Zorg voor een bericht van het bestuur dat MIVH-project grote prioriteit heeft en dat ieders bedrage welkom is;
- Zorg dat er medewerkers in het project komen met kennis van de processen en domeinkennis van de veiligheidsvraagstukken;
- Overweeg training en workshops als middel om betrokkenheid van medewerkers bij het proces te vergroten;
- De betrokkenheid en eigenaarschap op het MIVH wordt vergroot door interactieve communicatie met interne en externe belanghebbenden;
- Monitor regelmatig de voortgang;
- Pas de aanpak aan als dat nodig is;
- Communiceer met opdrachtgever en stakeholders;
- Bouw en communiceer op de (kleine) successen;
- Betrokkenheid en eigenaarschap groeit met successen.

Het volgende raamwerk is een VOORBEELD en kan als basis worden gebruikt voor het plannen van de benodigde activiteiten om het MIVH te implementeren.

1. Project Planning implementatie MIVH

	Doel	Acties	Deelnemers	Resultaat	Planning
1A	Verkrijg top-level ondersteuning, commitment en deelname voor MIVH	Maak instemming met MIVH een agendapunt voor CvB. Wie wordt (vooralsnog) portefeuillehouder veiligheid in CvB en welke senior manager wordt trekker?	• CvB • Manager XXX •	Akkoord van CvB om MIVH project te starten	Datum
1B	Benoem MIVH projectleider	CvB benoemt projectleider	• CvB • Manager XXX	XXX is projectleider	Datum
1C	Bemens MIVH team	Zet vraag uit bij managers en pols animo van gegadigden. Zorg voor spreiding binnen de instelling.	• Manager XXX • Managers • MIVH projectleider •	De leden van het projectteam	Periode
1D	Stel begeleidingscommissie en randvoorwaarden vast om MIVH project te begeleiden	Wijs commissieleden aan, stel taken, bevoegdheden en vergaderfrequentie van de commissie vast. Waarborg betrokkenheid en inspanningsverplichting van de commissieleden.	• Manager XXX • Manager Kwaliteit • MIVH projectleider •	Mandaat en leden van de commissie	Datum
1E	Train de projectleden en begeleidingscommissie in MIVH	Regel een training, toegesneden op beide doelgroepen, nodig deelnemers uit, zie toe op het volgen van de training	• MIVH team • MIVH commissieleden • Trainer / consultant •	MIVH Projectteam en begeleidingscommissie zijn opgeleid voor MIVH taken	periode
1F					

2. MIVH Strategische omgeving

	Doel	Acties	Deelnemers	Resultaat	Planning
2A	MIVH moet stroken met strategische doelen van de instelling.	Bestuur zal met de commissie de strategische doelen en plannen bijstellen.	• Manager XXX • MIVH Commissie • MIVH projectleider •	MIVH strategische doelen zijn in de strategie van de instelling verwerkt.	
2B	CEO onderschrijft de doelstelling om met het MIVH integraal de veiligheidsrisico's te beheersen.	Stel procedure op om MIVH in de bedrijfsvoering te integreren.	• CvB • Manager XXX • Projectleider MIVH	Management statement voor MIVH in te stellen	
2C	Gemeenschappelijk kader en terminologie voor MIVH toespitsen op de instelling.	Laat een aantal MIVH projectleden dit voorbereiden.	• MIVH team	1. Werkgroep die MIVH toespitst op de instelling 2. Eigen MIVH kader	
2D	Ontwikkel bewustzijn in de instelling voor veiligheidsrisico's, veilig gedrag en inventariseer het niveau van risico acceptatie.	Projectteam evalueert bestaande risicorapportages, -evaluaties en beleidsdocumenten.	• MIVH team • MIVH Commissie •	Niveau van risico acceptatie van de instelling is vastgesteld.	
2^{E}			•		

3. Maak een raamwerk voor evaluatie en prioritering van risico's

	Doel	Acties	Deelnemers	Resultaat	Planning
3A	Ontwikkel een portfolio van relevant risico's voor de instelling.	1. Inventariseer, evalueer en categoriseer een eerste 100 risico's in een risico matrix (impact en kans). 2. Selecteer 10-20 risico's om te mitigeren. 3. Herhaal deze activiteit periodiek.	• MIVH team	Meest relevant risico's voor de instelling om te mitigeren.	
3B	Ontwikkel een methodes of tools voor risico identificatie en evaluatie die medewerkers in het dagelijks werk kunnen gebruiken.	Inventariseer welke methodes of tools al worden gebruikt. Bepaal of die breder inzet baar zijn. Pas die eventueel aan.	• MIVH team	Hulpmiddelen voor dagelijks gebruik in de instelling om zelf risico's te kunnen duiden en prioriteren en om mitigerende maatregelen te kunnen overwegen.	
3C			•		

4. Review het proces van risicobeheersing

	Doel	Acties	Deelnemers	Resultaat	Planning
4A	Zekerstellen dat alle mitigerende initiatieven zijn afgestemd en bijdragen aan het geaccepteerde risiconiveau.	Selecteer de optimale strategieën en maatregelen om de geprioriteerde risico's te mitigeren.	• MIVH team • MIVH commissie • Ondernemingsraad •	Bestuur en beleidmakers worden ondersteund in het managen van risico's.	
4B	Voortgang van het risicomanagement proces bevorderen en vaststellen.	Monitor, evalueer en geef feedback op voorgestelde strategieën en mitigerende maatregelen.	• MIVH commissie • CvB •	Risk management initiatieven worden uitgevoerd.	Doorlopend
4C	Borg het MIVH proces zodat de hele instelling betrokken raakt en zich verantwoordelijk voelt voor het managen van risico's.	Integreer MIVH processen met bestaande bedrijfsvoering Stel aanvullende procedures op voor implementeren van MIVH	• MIVH commissie • CvB • MIVH team	Ontkokering van veiligheidssilo's MIVH proces geïntegreerd in de organisatie	
4D			•		

5. Ontwikkel een systeem voor MIVH communicatie, monitoring en verantwoording

	Doel	Acties	Deelnemers	Resultaat	Planning
5A	Communicatiestrategie en uitvoering voor MIVH	Stel werkgroep voor MIVH promotie/ communicatie in. Bepaal de taken en randvoorwaarden van deze groep.	• MIVH team	Deskundige werkgroep die de promotie en communicatie over veiligheid op zich neemt.	
5B	Communicatiestrategie en uitvoering voor MIVH	Presenteer MIVH informatie bij RvC, strategische bijeenkomsten, ondernemingsraad, nieuwe medewerkers, studenten,	• MIVH team	Bewustwording op MIVH in de hele instelling en omgeving.	
5C	Communicatiestrategie en uitvoering voor MIVH	Ontsluit MIVH informatie via de website van de instelling.	• MIVH team • Afd. communicatie	Informatie over MIVH is voor iedereen onder handbereik.	
5D	Communicatiestrategie en uitvoering voor MIVH	Schrijf artikelen voor nieuwsbrieven en dergelijke.	• MIVH team • Afd. communicatie	Bewustwording en educatie van alle medewerkers over MIVH.	
5E	Monitoring en verantwoording	Ontwikkel KPI's voor monitoring en verbetering van MIVH.	• MIVH team •	MIVH wordt meetbaar en beheersbaar.	
5F	Monitoring en verantwoording	Ontwikkel trainingsprogramma en toolset voor monitoring en verantwoording MIVH.	• MIVH team •	Alle medewerkers zijn getraind in het omgaan met veiligheidsrisico's en beschikken over tools om risico's te analyseren en daarover te rapporteren.	
5G	Monitoring en verantwoording	Houdt MIVH Table-top oefeningen en crisismanagement-oefeningen	• MIVH team • MIVH commissie • Management	MIVH doelen worden bijgesteld en MIVH wordt voortdurend verbeterd.	
5H	Monitoring en verantwoording	Maak jaarrapportage voor CvB en RvT over MIVH.	• MIVH team • MIVH commissie • Management	Verantwoording wordt afgelegd over MIVH doelen en resultaten.	
5I			•		

Bijlage 3: Relaties tussen dreigingen, te beschermen belangen en veiligheidsthema's

Ieder veiligheidsvraagstuk kan worden ontbonden in een te beschermen belang, dreigingen op dit belang en maatregelen op de bescherming van het belang.

Daarnaast is het essentieel om het krachtenspel van betrokkenen goed in het vizier te hebben. Dat zijn in eerste instantie alle belanghebbenden bij de te beschermen belangen. Wie zijn deze belanghebbenden en wat voor type belangen hebben zij? Vanuit de maatregeleninvalshoek zijn ook de betrokkenen identificeerbaar. Zij dienen de procedures goed uit te voeren en over voldoende kennis en kunde te beschikken. Ook zal bij sommige maatregelen een afweging gemaakt moeten worden op verschillende belangen (bijvoorbeeld cameratoezicht: privacy versus sociale veiligheid). Via de dreigingsanalyse komen de actoren die een dreiging kunnen veroorzaken in beeld.

Top-down is het nuttig om te sturen op veiligheidsthema's. De veiligheidsthema's worden dan op het hoogste niveau belegd en met programma's en aanpakken ingevuld. Bij de praktische invulling wordt echter direct tegen de grote verwevenheid van belangen, dreigingen en maatregelen/aanpakken aangelopen. De tien benoemde veiligheidsthema's hebben vanuit hun benaming het volgende vertrekpunt:

Veiligheidsthema	*Belang*	*Dreiging*	*Maatregel*
Integrale aanpak / Governance, Risk, Compliance			X
Arbeidsomstandigheden	X		
Milieu	X		
Sociale veiligheid	X		
Integriteit	X		
Informatieveiligheid	X		
Privacy	X		
Spionage / kennisveiligheid	X	X	
Internationalisering	X		
Gebouwveiligheid	X		
Crisismanagement, BHV, BCM	X		X

Hiermee is nog steeds geen concreet beeld op de te beschermen belangen, de type dreigingen die worden voorzien en de hoofdtypen van maatregelen.

<u>Breakdown van belangen en dreigingen en relaties met veiligheidsthema's</u>
In de volgende overzichten worden de volgende relaties gelegd:

- Belangen en dreigingen

- Belangen en veiligheidsthema's
- Dreigingen en veiligheidsthema's

Dit betreft een eerste startpunt. Een instelling dient dit verder concreet te maken.

	Te beschermen belangen	Mensen	Mensen in buitenland	Buitenlanders in NL	Kennis	Persoonsgegevens	Overige informatie	ICT	Examen registratie	Inkoop proces	Financien proces	Gebouwen	Laboratoria, werkplaatsen, apparatuur, opstellingen	Nucleaire installatie	Proefdieren
Waar tegen te beschermen															
Organisatorisch/technisch falen															
Brand		x		x				x				x	x	x	x
Uitval															
Uitval energie								x				x	x	x	x
Uitval externe ICT								x							
Falen op afval, asbest, chemie, radiologisch, nucleair proc		x										x	x	x	
Falen op dierverzorging		x													x
Falen gebouwinstallaties												x	x	x	x
Falen verkeersafhandeling		x										x			
Falen evenement/crowd control		x										x			
Falen voedselvoorziening		x													
Moedwillig handelen															
Diefstal															
Insluiping en inbraak (fysiek en digitaal)			?	?				x				x	x	x	x
Diefstal goederen en informatie		x	x	x	x	x	x	x	x	x	x	x	x	x	x
Fraude					x	x			x	x	x		x		
Spionnage		x	x	x	x	x			x	x					
Cyberaanval		x	x	x		x		x							
Geweld															
Pestgedrag		x	x	x		x		x				x			
Bedreiging en intimidatie		x	x	x		x									
Afpersing en chantage		x	x	x		x									
Ernstige (fysieke) bedreiging		x	x	x								x	x	x	x
Gijzeling, ontvoering			x												
Openbare orde															
Bezetting, blokkade, protest												x	x	x	x
Sabotage															
Kleine vernielingen		x						x				x	x	x	x
Brandstichting												x	x	x	x
Molest aan gebouw												x	x	x	x
Overig															
Opblazen en beschieten		x	x	x								x	x	x	x
(nep) bombrief, b/c brief		x										x			
Nalatigheid en non discipline															
Ernstige nalatigheid		x	x	x	x	x	x	x	x	x	x	x	x	x	x
Negeren rookverbod		x										x	x	x	x
Negeren parkeervoorschriften		x										x			
Externe dreigingen															
Extreme wateroverlast, sneeuw, ijs		x						x				x	x	x	x
Extreme hitte, kou		x						x				x	x	x	x

	Veiligheidsthema	Governance, risk, compliance	Arbeidsomstandigheden	Milieuveiligheid	Sociale veiligheid	Integriteit	Informatieveiligheid	Privacy	Kennisveiligheid/ spionnage	Internationalisering	Gebouwveiligheid	Crisismanagement, BHV, BCM
Waar tegen te beschermen												
Organisatorisch/technisch falen												
Brand		x	x	x			x				x	x
Uitval												
Uitval energie		x					x				x	x
Uitval externe ICT		x					x					x
Falen op afval, asbest, chemie, radiologisch, nucleair proc		x	x	x							x	x
Falen op dierverzorging		x	x	x							x	x
Falen gebouwinstallaties		x	x		x						x	x
Falen verkeersafhandeling		x			x						x	x
Falen evenement/crowd control		x			x						x	x
Falen voedselvoorziening		x	x									x
Moedwillig handelen												
Diefstal												
Insluiping en inbraak (fysiek en digitaal)		x	x		x		x		x	x	x	x
Diefstal goederen en informatie		x	x		x		x	x	x	x	x	x
Fraude		x				x	x		x			x
Spionnage		x					x		x	x		x
Cyberaanval		x			x		x		x			x
Geweld												
Pestgedrag		x	x		x			x		x		x
Bedreiging en intimidatie		x	x		x			x		x		x
Afpersing en chantage		x	x		x			x		x		x
Ernstige (fysieke) bedreiging		x			x					x		x
Gijzeling, ontvoering		x	x		x					x		x
Openbare orde												
Bezetting, blokkade, protest		x									x	x
Sabotage												
Kleine vernielingen		x			x						x	x
Brandstichting		x									x	x
Molest aan gebouw		x									x	x
Overig												
Opblazen en beschieten		x	x								x	x
(nep) bombrief, b/c brief		x	x								x	x
Nalatigheid en non discipline												
Ernstige nalatigheid		x	x	x	x	x	x	x	x	x	x	x
Negeren rookverbod		x	x								x	x
Negeren parkeervoorschriften		x									x	x
Externe dreigingen												
Extreme wateroverlast, sneeuw, ijs												
Extreme hitte, kou												

	Te beschermen belangen	Mensen	Mensen in buitenland	Buitenlanders in NL	Kennis	Persoonsgegevens	Overige informatie	ICT	Examen registratie	Inkoop proces	Financien proces	Gebouwen	Laboratoria, werkplaatsen, apparatuur, opstellingen	Nucleaire installatie	Proefdieren
Veiligheidsthema															
Governance, risk, compliance		x	x	x	x	x	x	x	x	x	x	x	x	x	x
Arbeidsomstandigheden		x	x	x								x	x	x	x
Milieu												x	x	x	x
Sociale Veiligheid		x	x	x				x							
Integriteit		x	x	x	x	x			x	x	x				
Informatieveiligheid		x	x	x	x	x	x	x	x	x	x		x	x	
Privacy		x				x									
Kennisveiligheid/spionnage		x	x	x	x				x	x					
Internationlisering			x	x											
Gebouwveiligheid												x	x	x	x
Crisismanagement, BHV, BCM		x	x	x	x	x	x	x	x	x	x	x	x	x	x

Colofon

Opdrachtgever:	Projectgroep Integrale Veiligheid Hoger Onderwijs
Projectcontact:	Paul Goossens (p.a.m.goossens@hr.nl)
Opgesteld door:	Joris Hutter en Marcel Spit (Adviescentrum BVI)
Bijdragen van:	Jeroen Terstegge (Privacy Management Partners) Alex Ivanovic (Adviesbureau Forta Nova)
Datum:	Mei 2014

Bijlage B

Zelfbeoordeling MIVH

INTEGRALE
VEILIGHEID
HOGER ONDERWIJS

Inhoudsopgave

Voorwoord 3

Voorbereiding 5

4 De instelling en zijn omgeving 5

4.1 Instelling en zijn omgeving 5

4.2 Behoeften en verwachtingen van partijen 5

4.3 Reikwijdte van het MIVH 5

4.4 MIVH 5

5 Leiderschap 5

5.1 Leiderschap en betrokkenheid 5

5.2 MIVH-beleid 6

5.3 Verantwoordelijkheden en bevoegdheden 6

Plan 6

6 Planvorming 6

6.1 Risico en impact analyse 6

6.2 Doelen en thema's 7

7 Ondersteuning 7

7.1 Middelen 7

7.2 Competenties 7

7.3 Bewustzijn 8

7.4 Communicatie 8

7.5 Gedocumenteerde informatie 8

Do 8

8 Werking 8

8.1 Operationele planvorming en beheersing - algemeen 8

8.2 Arbeidsomstandigheden 9

8.3 Milieuveiligheid 9

8.4 Sociale veiligheid 10

8.5 Integriteit 10

8.6 Informatieveiligheid 11

8.7 Privacy 11

8.8 Kennisveiligheid 11

8.9 Internationalisering 12

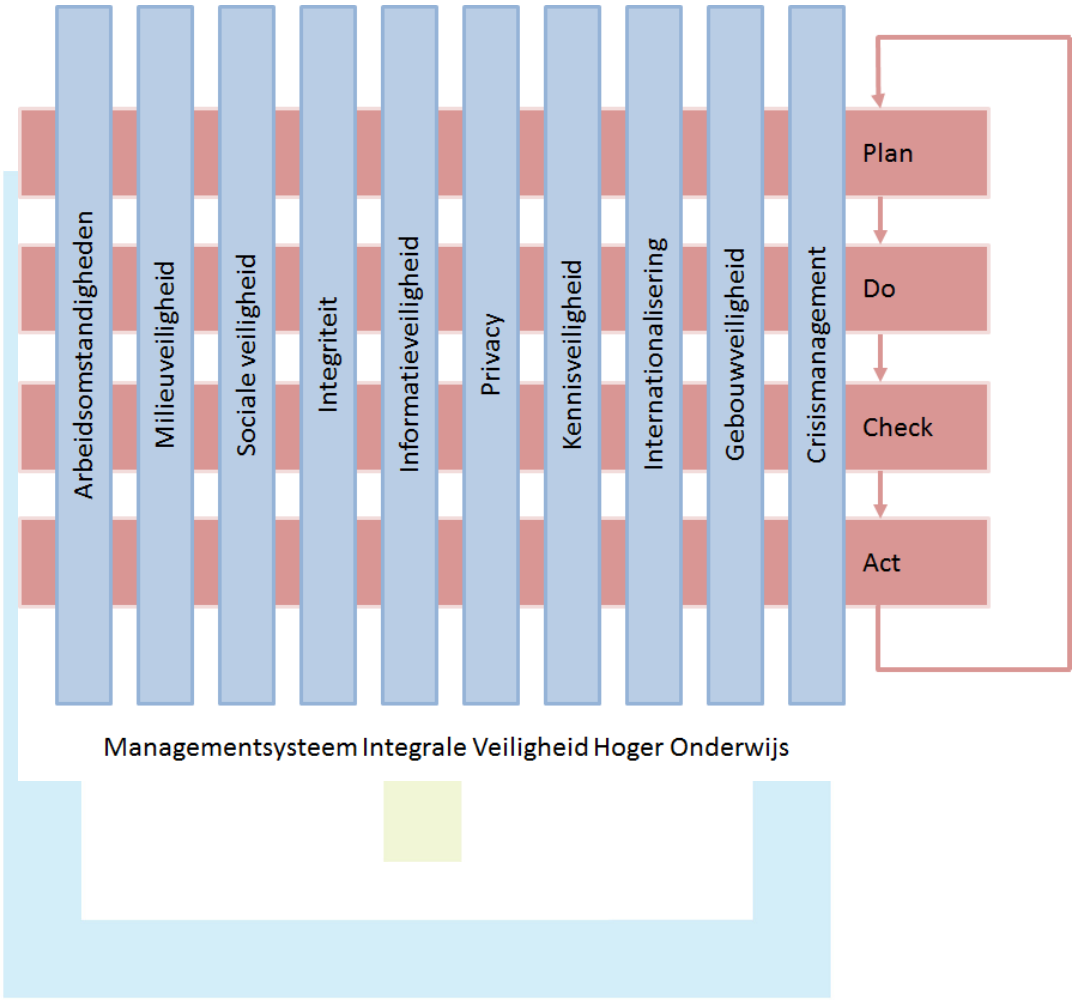
8.10 Gebouwveiligheid 13
8.11 Crisismanagement, BHV, BCM 14
Check 14
9 Evaluatie van de werking 14
9.1 Bewaking, meting, analyse en evaluatie 14
9.2 Interne audits 14
9.3 Management review 15
Act 15
10 Verbetering 16
10.1 Non-conformiteiten en corrigerende acties 16
10.2 Voortdurende verbetering 16
Colofon 17

Voorwoord

Voorliggend document bevat vragen aan de hand waarvan een instelling kan nagaan in hoeverre de betreffende onderdelen van een integraal managementsysteem op veiligheid aandacht behoeven, voldoende op orde zijn en aantoonbaar geborgd zijn.

Ontwikkeling van Managementsysteem Integrale Veiligheid Hoger Onderwijs (MIVH)
Het project 'Integraal Veilig Hoger Onderwijs' beoogt instellingen in het hoger onderwijs te ondersteunen bij het integraal omgaan met veiligheidsvraagstukken door expertise te bundelen, samen op te trekken en handreikingen te bieden om risico's te monitoren, beheersbaar te maken en te houden.

In het deelproject 'Governance' is een 'Managementsysteem Integrale Veiligheid Hoger Onderwijs' (MIVH) gedefinieerd als hulpmiddel om sturing te geven op integrale veiligheid. Het MIVH is direct afgeleid van de High Level Structure voor managementsystemen en volgt de PDCA-cyclus die binnen alle managementsystemen van ISO aanwezig is. Verschillende managementsysteemnormen, maar ook eigen instellingsnormen kunnen hier eenvoudig op worden 'ingeplugd'. Vanuit management optiek is er logischerwijs behoefte aan één managementsysteem om integraal alle veiligheidsaspecten van een organisatie te beheren. In het project zijn tien veiligheidsthema's gedefinieerd.



Er zijn drie documenten/instrumenten op MIVH ontwikkeld als hulpmiddel en inspiratie voor instellingen die een verbeterslag willen maken op veiligheid:

1. Het Managementsysteem Integrale Veiligheid Hoger Onderwijs (MIVH). Het kerndocument is opgesteld in een vorm van toetsbare elementen (eisen stellen document).
2. Een handleiding op het MIVH. De handleiding geeft aanpakken op het MIVH en gaat in op de verschillende veiligheidsthema's van een instelling. In de handleiding zijn verwijzingen opgenomen naar diverse bruikbare aanpakken en normen op die veiligheidsthema's.
3. Zelfbeoordelingsinstrument. Dit betreft een vragenlijst die bruikbaar is als zelfbeoordeling op MIVH.

Dit document betreft de vragenlijst ten behoeve van de zelfbeoordeling.

Gebruik van deze vragenlijst
Deze vragenlijst volgt de hoofstukindeling van het MIVH. Dit MIVH start met enkele inleidende hoofdstukken. Vanaf hoofdstuk 4 worden eisen gesteld aan het managementsysteem. Daarom start deze vragenlijst ook pas bij hoofdstuk 4.

Overige instrumenten
Naast voorliggende vragenlijst zijn er ook andere aanvullende instrumenten die bruikbaar zijn voor zelfbeoordeling op onderdelen van de veiligheidsaanpak:

- SURF, Normenkader, assessments en benchmark. Dit betreft een normenkader gebaseerd op ISO27002 op informatiebeveiliging, continuïteit van bedrijfsgegevens en privacy.
- Integrale Veiligheid Hoger Onderwijs, SAINT (self assessment integriteit). Dit betreft een beoordelingsinstrument op de terreinen van integriteit, kennisveiligheid en informatieveiligheid. Hierop is tevens een Group Decision Room Applicatie 'IRMA' (integraal of integriteit risico management assessment app) gebaseerd.

Verdere ontwikkeling van dit beoordelingsinstrument
Dit is een eerste versie is van een beoordelingsinstrument op integrale veiligheid. Wij zien hierbij een inhoudelijke ontwikkeling op type vragen. Zijn er vragen die overbodig zijn? Zijn er aspectgebieden die nog niet goed bevraagd worden? Kan de vraagstelling duidelijker?
Daarnaast zal de vragenlijst naar een tooling worden gebracht, zodat deze als een zelfbeoordelingsinstrument kan worden gebruikt, maar ook als een instrument voor externe beoordeling. Tenslotte zouden de vragen ook gebruikt kunnen worden in een nader te bepalen vorm van benchmark vergelijking.
Voor bovenstaande zijn feedback en suggesties vanuit de instellingen zeer welkom. In een volgend initiatief van de projectgroep integrale veiligheid kan het toetsingsinstrument hier verder op worden ontwikkeld en getest.

De deelprojectgroep Governance.

Voorbereiding

4 De instelling en zijn omgeving

4.1 Instelling en zijn omgeving

1. Zijn in- en externe onderwerpen vastgesteld die van belang zijn voor het vervullen van zijn missie?
2. Zijn in- en externe onderwerpen vastgesteld die van belang zijn voor het vervullen van zijn doelstelling,
3. Zijn in- en externe onderwerpen vastgesteld die van belang zijn voor het vervullen van zijn visie?
4. Zijn in- en externe onderwerpen vastgesteld die van belang zijn voor het vervullen van zijn verantwoordelijkheid?

4.2 Behoeften en verwachtingen van partijen

5. Zijn de belanghebbenden voor MIVH vastgelegd?
6. Zijn de behoeften van de belanghebbenden vastgelegd?

4.3 Reikwijdte van het MIVH

7. Is er een verklaring van toepasselijkheid vastgesteld?
8. Zijn hierin de in- en externe onderwerpen uit 4.1 opgenomen?
9. Zijn hierin de behoeften van de belanghebbenden uit 4.2 opgenomen?

4.4 MIVH

10. Heeft de instelling een MIVH?
11. Wordt het MIVH onderhouden en continu verbeterd?

5 Leiderschap

5.1 Leiderschap en betrokkenheid

12. Draagt de hoogste leiding zorg voor dat het MIVH-beleid en de MIVH-doelen worden vastgesteld en in overeenstemming zijn met de strategische koers van de instelling?
13. Draagt de hoogste leiding zorg voor dat de MIVH-eisen worden geïntegreerd in de reguliere processen van de instelling?
14. Draagt de hoogste leiding zorg voor dat de middelen die nodig zijn voor MIVH, beschikbaar zijn?
15. Draagt de hoogste leiding een effectieve MIVH en naleving van MIVH-eisen uit?
16. Draagt de hoogste leiding zorg voor dat MIVH de beoogde resultaten bereikt?
17. Steunt en stuurt de hoogste leiding personen in het bijdragen aan de effectiviteit van MIVH?
18. Draagt de hoogste leiding continue verbetering actief uit?
19. Zorgt de hoogste leiding ervoor dat andere managementniveaus leiderschap tonen binnen hun gebieden van verantwoordelijkheid?

20. Draagt de hoogste leiding zorg voor afstemming met interne organen voor inspraak en medezeggenschap?
21. Draagt de hoogste leiding zorg voor handhaving en naleving van wettelijke en branche regulering verplichtingen?
22. Draagt de hoogste leiding zorg voor rechtsbescherming studenten en personeel in de vorm van regelingen beroep en bezwaar?

5.2 MIVH-beleid

23. Heeft de hoogste leiding van de instelling het MIVH-beleid vastgesteld?
24. Is het MIVH-beleid passend voor de doelstelling van de instelling?
25. Biedt het MIVH-beleid een raamwerk voor het kunnen vaststellen van de MIVH-doelen?
26. Bevat het MIVH-beleid een zelfverplichting om te voldoen aan de van toepassing zijnde eisen?
27. Bevat het MIVH-beleid een zelfverplichting om MIVH voortdurend te verbeteren?
28. Is het MIVH-beleid beschikbaar als officieel vastgesteld document?
29. Is het MIVH-beleid bekend gemaakt binnen de instelling?
30. Is het MIVH-beleid beschikbaar voor belanghebbenden, voor zover van toepassing.

5.3 Verantwoordelijkheden en bevoegdheden

31. Draagt de hoogste leiding ervoor zorg dat verantwoordelijkheden en bevoegdheden voor relevante rollen worden toegewezen?
32. Heeft de hoogste leiding deze verantwoordelijkheden en bevoegdheden bekend gemaakt binnen de instelling?
33. Is bij de toewijzing van verantwoordelijkheden en bevoegdheden ervoor gezorgd dat MIVH zich conformeert aan de eisen van deze norm?
34. Is bij de toewijzing van verantwoordelijkheden en bevoegdheden ervoor gezorgd dat de hoogste leiding voortdurend op de hoogte wordt gesteld van de ten uitvoer legging van MIVH?

Plan

6 Planvorming

6.1 Risico en impact analyse

35. Is er een plan voor de implementatie van MIVH?
36. Zijn alle onderwerpen uit 4.1 verwerkt in het plan?
37. Zijn alle eisen uit 4.2 verwerkt in het plan?
38. Is in het plan rekening gehouden met kansen en risico's met betrekking tot het realiseren van het doel van MIVH?
39. Zijn deze kansen/risico's vertaald in acties in het MIVH-implementatieplan?
40. Worden deze acties geëvalueerd op effectiviteit?
41. Is in het plan rekening gehouden met kansen en risico's met betrekking tot ongewenste effecten?
42. Zijn deze kansen/risico's vertaald in acties in het MIVH-implementatieplan?
43. Worden deze acties geëvalueerd op effectiviteit?

44. Is in het plan rekening gehouden met kansen en risico's met betrekking tot het realiseren van continue verbetering?
45. Zijn deze kansen/risico's vertaald in acties in het MIVH-implementatieplan?
46. Worden deze acties geëvalueerd op effectiviteit?
47. Zijn de acties verankerd in de bedrijfsvoeringprocessen?
48. Maken deze acties deel uit van het interne kwaliteitszorgsysteem?

6.2 Doelen en thema's

49. Zijn de MIVH-doelen op relevante niveaus en functies vastgesteld?
50. Zijn de MIVH-doelen consistent met het MIVH-beleid?
51. Zijn de MIVH-doelen meetbaar?
52. Is bij de MIVH-doelen rekening gehouden met van toepassing zijnde eisen?
53. Worden de MIVH-doelen bewaakt?
54. Worden de MIVH-doelen uitgedragen?
55. Worden de MIVH-doelen bijgewerkt indien nodig?
56. Wordt informatie met betrekking tot de MIVH-doelen gedocumenteerd?
57. Is bij het plannen hoe de MIVH-doelen zullen worden bereikt, vastgesteld wat dient te gebeuren?
58. Is bij het plannen hoe de MIVH-doelen zullen worden bereikt, vastgesteld welke middelen daarvoor nodig zijn?
59. Is bij het plannen hoe de MIVH-doelen zullen worden bereikt, vastgesteld wie voor de uitvoering verantwoordelijk is?
60. Is bij het plannen hoe de MIVH-doelen zullen worden bereikt, vastgesteld wanneer het volbracht dient te zijn?
61. Is bij het plannen hoe de MIVH-doelen zullen worden bereikt, vastgesteld hoe de resultaten dienen te worden beoordeeld?

7 Ondersteuning

7.1 Middelen

62. Is vastgesteld welke middelen nodig zijn om het MIVH te ontwikkelen?
63. Is vastgesteld welke middelen nodig zijn om het MIVH te implementeren?
64. Is vastgesteld welke middelen nodig zijn om het MIVH te onderhouden?
65. Is vastgesteld welke middelen nodig zijn om het MIVH te voortdurend te verbeteren?
66. Zijn die middelen beschikbaar gesteld?

7.2 Competenties

67. Zijn de vereiste competenties van personeel die de uitvoering van MIVH (kunnen) beïnvloeden vastgesteld?
68. Is zeker gesteld dat deze personen competent zijn op grond van hun opleiding, training en/of ervaring?
69. Indien van toepassing: wordt actie ondernomen om de noodzakelijke competenties te verwerven en de affectiviteit van deze actie te evalueren?
70. Wordt relevante documentatie bewaard als bewijs van competenties?
71. Beschikt de instelling over relevante functieprofielen en functionarissen?

7.3 Bewustzijn

72. Personeel en studenten zijn zich bewust van het MIVH-beleid?
73. Personeel en studenten zijn zich bewust van de van hen verwachte bijdrage aan de effectiviteit van MIVH, met inbegrip van de voordelen van een verbeterde MIVH uitvoering?
74. Personeel en studenten zijn zich bewust van de gevolgen van niet-naleving van de MIVH-eisen?

7.4 Communicatie

75. Is de noodzaak van in- en externe communicatie die relevant is voor MIVH vastgesteld?
76. Is daarbij vastgesteld waarover moet worden gecommuniceerd?
77. Is daarbij vastgesteld wanneer moet worden gecommuniceerd?
78. Is daarbij vastgesteld aan wie de communicatie moet worden gericht?

7.5 Gedocumenteerde informatie

79. Omvat het MIVH gedocumenteerde informatie die krachtens deze norm verplicht is?
80. Omvat het MIVH gedocumenteerde informatie die de instelling heeft aangegeven als noodzakelijk voor de effectiviteit van het MIVH?
81. Is bij het maken/bewerken van gedocumenteerde informatie zorggedragen voor identificatie en beschrijving (bijvoorbeeld titel, datum, auteur of referentienummer)?
82. Is bij het maken/bewerken van gedocumenteerde informatie zorggedragen voor formaat (bijvoorbeeld taal, software versie, figuren) en media (bijvoorbeeld op papier of elektronisch)?
83. Is bij het maken/bewerken van gedocumenteerde informatie zorggedragen voor beoordeling en goedkeuring qua geschiktheid en is dat toereikend?
84. Wordt de gedocumenteerde informatie beheerd?
85. Zorgt het beheer ervoor dat het beschikbaar en geschikt is voor gebruik, op de plaats en tijd waar het nodig is?
86. Zorgt het beheer ervoor dat het afdoende is beveiligd (bijvoorbeeld tegen schending van vertrouwelijkheid, onjuist gebruik of verlies van integriteit)?
87. Richt het beheer zich op activiteiten omtrent verspreiding, toegang, opvraging en gebruik?
88. Richt het beheer zich op activiteiten omtrent opslag en behoud, met inbegrip van behoud van leesbaarheid?
89. Richt het beheer zich op activiteiten omtrent beheer van wijzigingen (bijvoorbeeld versiebeheer)?
90. Richt het beheer zich op activiteiten omtrent bewaartermijn en vernietiging?

Do

8 Werking

8.1 Operationele planvorming en beheersing - algemeen

91. Worden de processen gepland, geïmplementeerd en beheerst die nodig zijn om de eisen te vervullen en de acties die bepaald zijn in 6.1 te implementeren?
92. Zijn hierbij criteria voor de processen vastgesteld?
93. Is het beheer van de processen in overeenstemming met de criteria geïmplementeerd?

94. Wordt de gedocumenteerde informatie bijgehouden voor zover nodig om vertrouwen te hebben dat de processen zijn uitgevoerd zoals gepland?
95. Worden geplande wijzigingen beheerst?
96. Worden de gevolgen van ongeplande wijzigingen beoordeeld en daarbij acties uitgevoerd om negatieve gevolgen te mitigeren?
97. Is er zorg voor gedragen dat uitbesteedde processen worden beheerst?

8.2 Arbeidsomstandigheden

98. Heeft uw instelling een coördinator op arbeidsomstandigheden?
99. Is arbeidsomstandigheden belegd in één van de portefeuilles van het College van Bestuur?
100. Is binnen uw instelling voldoende kennis aanwezig op arbeidsomstandigheden?
101. Heeft uw instelling een beleid op arbeidsomstandigheden?
102. Kan uw instelling zich verantwoorden op een gepaste omgang met arbeidsomstandigheden?
103. Voldoet uw instelling aan de eisen van de Arbeidsomstandighedenwet?
104. Worden onveilige arbeidsomstandigheden zoals gladheid, niet-stabiele ondergrond, omvallende objecten, blootstelling aan hoge voltages, dampen, stralingen, bacteriën of virussen actief vermeden?
105. Stelt uw instelling gezonde werkplekken ter beschikking?
106. Monitort en stuurt uw instelling op arbeidsverzuim?
107. Zijn risicovolle locaties afgeschermd en is er toegangsbeheersing?
108. Zijn er voor risicovolle werkzaamheden heldere gedragsregels, trainingen en voorlichting?
109. Zijn er een klachtenregeling en een vertrouwenspersoon c.q. ombudsman voor personeel en voor studenten?
110. Is een klokkenluidersregeling aanwezig?
111. Werkt uw instelling met uit de VSNU Arbocatalogus (www.vsnu.nl/arbocatalogus.html)
112. Werkt uw instelling met alle relevante onderdelen uit de VH Arbocatalogus (www.arbocatalogushbo.nl)
113. Werkt uw instelling volgens de NPR 5001 - Model voor een arbo-managementsysteem.
114. Werkt uw instelling volgens de NTA 8031 - Registratie van arbeids- en bedrijfsongevallen.

8.3 Milieuveiligheid

115. Heeft uw instelling een coördinator op milieuveiligheid?
116. Is milieuveiligheid belegd in één van de portefeuilles van het College van Bestuur?
117. Is binnen uw instelling voldoende kennis aanwezig op milieuveiligheid?
118. Heeft uw instelling een beleid op milieuveiligheid?
119. Kan uw instelling zich verantwoorden op een gepaste omgang met milieuveiligheid?
120. Heeft uw instelling een verantwoordbaar beleid op energiebelasting?
121. Heeft uw instelling een verantwoordbaar beleid op belasting van riolering, oppervlaktewater, scheiding van afvalstromen?
122. Heeft uw instelling maatregelen op legionella?
123. Heeft uw instelling maatregelen op asbest?
124. Kent uw instelling radiologische bronnen, heeft uw instelling een radiologisch veiligheidsfunctionaris en kan uw instelling zich op dit thema verantwoorden?
125. Kent uw instelling biosafety of diermicro labs, heeft uw instelling een biologische veiligheidsfunctionaris en kan uw instelling zich op dit thema verantwoorden?
126. Heeft uw instelling alle milieuvergunningen?

8.4 Sociale veiligheid

127. Heeft uw instelling een coördinator op sociale veiligheid?
128. Is sociale veiligheid belegd in één van de portefeuilles van het College van Bestuur?
129. Is binnen uw instelling voldoende kennis aanwezig op sociale veiligheid?
130. Heeft uw instelling een beleid op sociale veiligheid?
131. Kan uw instelling zich verantwoorden op een gepaste omgang met sociale veiligheid c.q. wordt aandacht gegeven aan een of meer van de onderstaande onderwerpen?
    a) Beschikt uw instelling over handreikingen m.b.t. sociale veiligheid?
    b) Beschikt uw instelling over de handreiking voor signalering en aanpak van veiligheid en leefstijlrisico's in het HBO?
    c) Beschikt uw instelling over de handreiking preventie en omgaan met schoolaanslagen
    d) Informatieblad voor schietpartijen op scholen
    e) Agressie tegen personeel
    f) Agressieve leerlingen
    g) Agressieve ouders
    h) Discriminatie en racisme
    i) Online pesten
    j) Seksuele intimidatie
    k) Wapengeweld
    l) Burgerschap
    m) Conflictbemiddeling
    n) Gedrag en kleding
    o) Peers
    p) Sociale competenties
    q) Weerbaarheid
    r) Seksuele diversiteit
    s) Huiselijk geweld
    t) Seksueel geweld in de thuissituatie
    u) Eerwraak en huwelijksdwang
    v) Extremisme en radicalisering
    w) Fysieke veiligheid
    x) Veiligheid en handicap
    y) Drugs op school
    z) Mediawijsheid
132. Is uw instelling betrokken bij het kennisplatform Veilige Publieke Taak Onderwijs (www.forumveiligeschool.nl)?
133. Heeft uw instelling expertise ontwikkeld hoe om te gaan met dreigingen op het terrein van radicalisering?
134. Is radicalisering bespreekbaar binnen uw instelling?
135. Is een vertrouwenspersoon/functionaris aangewezen in uw instellingen die alert is op signalen m.b.t. radicalisering
136. Is uw instelling alert op studenten die uit het buitenland terugkeren en er mogelijk radicale ideeën op nahouden?
137. Heeft u voorzieningen getroffen om daar melding over te maken?

8.5 Integriteit

138. Heeft uw instelling een coördinator op integriteit?
139. Is integriteit belegd in één van de portefeuilles van het College van Bestuur?

140. Is binnen uw instelling voldoende kennis aanwezig op integriteit?
141. Beschikt uw instelling over een integriteitsbeleid en gedragscodes voor integer handelen?
142. Heeft uw instelling beleid ten aanzien van wetenschappelijke integriteit geborgd?
143. Verantwoordt uw instelling zich over het gevoerde integriteitsbeleid?
144. Wordt de professionaliteit, betrouwbaarheid, onkreukbaarheid en zorgvuldigheid van uw instelling geborgd?
145. Wordt aan de integriteit van medewerkers, bestuurders, docenten en studenten gewerkt?
146. Wordt wetenschapsfraude en plagiaat door onderzoekers bestreden?
147. Wordt fraude door medewerkers en zelfverrijking en ongewenst declaratiegedrag door bestuurders en managers aangepakt?
148. Heeft uw instelling een actieve aanpak op examen/tentamenfraude?
149. Heeft uw instelling een gedragscode waarin de omgang met dilemma's en normen voor afwijkend gedrag zijn beschreven?
150. Is een vertrouwenspersonen Integriteit aangesteld?
151. Is een gedragsnorm goed bestuur en integriteit opgesteld?
152. Heeft uw instelling een meldprocedure voor vermoedens van misstanden?
153. Heeft uw instelling een protocol voor het onderzoeken van integriteitsschendingen?
154. Doet uw instelling bij (vermoeden van) strafbare feiten aangifte bij de politie of de officier van justitie?
155. Legt uw instelling jaarlijks aan de Raad van Toezicht verantwoording af over het gevoerde integriteitsbeleid?
156. Werkt uw instelling met De Nederlandse Gedragscode Wetenschapsbeoefening, principes van goed wetenschappelijk onderwijs en onderzoek VSNU (2012)?

8.6 Informatieveiligheid

157. Heeft uw instelling een coördinator op informatieveiligheid?
158. Is informatieveiligheid belegd in één van de portefeuilles van het College van Bestuur?
159. Is binnen uw instelling voldoende kennis aanwezig op informatieveiligheid?
160. Heeft uw instelling een beleid op informatieveiligheid?
161. Kan uw instelling zich verantwoorden op een gepaste omgang met informatieveiligheid?
162. Wordt de informatiebeveiliging van uw instelling beoordeeld volgens het normenkader van SURF of een vergelijkbaar assessmentmodel?
163. Wordt de informatiebeveiliging hierbij als minimaal voldoende beoordeeld?

8.7 Privacy

164. Heeft uw instelling een privacy coördinator?
165. Is privacy belegd in één van de portefeuilles van het College van Bestuur?
166. Is binnen uw instelling voldoende kennis aanwezig op privacy?
167. Heeft uw instelling een privacy beleid?
168. Kan uw instelling zich verantwoorden op een gepaste omgang met persoonsgegevens?

8.8 Kennisveiligheid

169. Heeft uw instelling een coördinator op kennisveiligheid?
170. Is kennisveiligheid belegd in één van de portefeuilles van het College van Bestuur?
171. Is binnen uw instelling voldoende kennis aanwezig op kennisveiligheid?
172. Heeft uw instelling een beleid op kennisveiligheid?
173. Kan uw instelling zich verantwoorden op een gepaste omgang met kennisveiligheid?
174. Is in uw instelling voldoende aandacht voor het thema kennisveiligheid en bescherming van de cruciale belangen?

175. Is in uw instelling de beveiligingsorganisatie (de beveiligingsketen) ingericht? Zijn in uw instelling beveiligingstaken, -bevoegdheden en -verantwoordelijkheden aan de verschillende functionarissen toebedeeld?
176. Zijn bij uw instelling functies vastgesteld waarbij men in aanraking komt met de cruciale belangen van de instelling?
177. Worden in uw instelling medewerkers die in aanraking komen met cruciale belangen vóór indiensttreding gescreend?
178. Tekenen in uw instelling personeel en studenten die in aanraking komen met cruciale belangen een geheimhoudingsverklaring?
179. Is bij uw instelling kennisveiligheid en de bescherming van de cruciale belangen in het risicomanagementsysteem opgenomen?
180. Heeft uw instelling op een centrale plek informatie beschikbaar over kennisveiligheid en beveiligingsmaatregelen?
181. Wordt in uw instelling gecommuniceerd over aanpassingen van beveiligingsmaatregelen aan ontwikkelingen in de bedreigingen van de cruciale belangen?
182. Reageert uw instelling adequaat bij incidenten die de cruciale belangen schaden?
183. Draagt het bestuur van de instelling actief het belang van kennisveiligheid en bescherming van de cruciale belangen uit?
184. Heeft uw instelling de cruciale belangen geformuleerd en bekend gemaakt?
185. Zijn in uw instelling de risico's die cruciale belangen bedreigen geformuleerd en bekend gemaakt?
186. Is in uw instelling duidelijk welk persoonlijk handelen bijdraagt aan de bescherming van cruciale belangen?
187. Passen bestuurders, medewerkers en studenten van uw instelling de gedragingen die bijdragen aan de bescherming van cruciale belangen toe?
188. Beschikt uw instelling over een regeling voor de toegang tot en het omgaan met cruciale belangen binnen onze instelling?
189. Wordt in uw instelling (vertrouwelijke) informatie alleen uitgewisseld (fysiek en digitaal) als daarmee de cruciale belangen van de instelling niet worden geschaad?
190. Weten bestuur, management, medewerkers en studenten hoe ze vermoedens dat de cruciale belangen worden geschaad kunnen melden bij uw instelling?
191. Maakt bij uw instelling de bescherming van de cruciale belangen deel uit van de Plan & Control cyclus?
192. Heeft uw instelling activiteiten ontplooid om de bewustwording en alertheid van onderzoekers, medewerkers en studenten over kennisveiligheid te verhogen?
193. Gebruikt uw instelling een regeling op rubricering van informatie?
194. Gebruikt uw instelling een regeling op pattenteren?

8.9 Internationalisering

195. Heeft uw instelling een coördinator op veiligheidsaspecten bij internationalisering?
196. Is internationalisering belegd in één van de portefeuilles van het College van Bestuur?
197. Is binnen uw instelling voldoende kennis aanwezig op veiligheidsaspecten bij internationalisering?
198. Heeft uw instelling een beleid op internationalisering en veiligheid?
199. Kan uw instelling zich verantwoorden op een gepaste omgang met internationalisering en veiligheid?
200. Bereidt uw instelling studenten en medewerkers goed voor op mogelijk vreemde en risicovolle omstandigheden in het buitenland?

201. Is een procedure beschikbaar en zijn verwijzingen naar relevante documentatie actueel om je op de reis voor te bereiden?
202. Is iemand aangesteld om de veiligheid van de reizende te monitoren en om bij calamiteiten in te springen?
203. Wordt voldoende rekening gehouden met cultuur verschillen en afwijkende gewoontes en regelgeving?
204. Zijn de medische voorzieningen en primaire levensomstandigheden in kaart gebracht en is de reizende student of medewerker daarop voorbereid?
205. Is uw instelling voorbereid op de vermissing van een medewerker of student in het buitenland?
206. Heeft uw instelling buitenlandse bezoekers voldoende geïnformeerd over de situatie in Nederland, uw vestigingsplaats en instelling?
207. Is iemand aangewezen als vraagbaak en vertrouwenspersoon voor reizigers?
208. Beschikt uw instelling over een handreiking voor reizigers met informatie over afwijkende normen en regels in het buitenland, suggesties voor een goede reisvoorbereiding en vindplaats voor nadere informatie over relevante reisbestemmingen?
209. Beschikt uw instelling over een brochure in de Engelse taal voor bezoekende studenten en onderzoekers?
210. Gebruikt uw instelling de Gedragscode Internationale Student in het Nederlandse hoger onderwijs, opgesteld door het Nuffic?

8.10 Gebouwveiligheid

211. Heeft uw instelling een coördinator op gebouwveiligheid?
212. Is gebouwveiligheid belegd in één van de portefeuilles van het College van Bestuur?
213. Is binnen uw instelling voldoende kennis aanwezig op gebouwveiligheid?
214. Heeft uw instelling een beleid op gebouwveiligheid?
215. Kan uw instelling zich verantwoorden op een gepaste omgang met gebouwveiligheid?
216. Voldoen alle gebouwen van uw instelling aan het Bouwbesluit?
217. Voldoen alle gebouwen van uw instelling aan de relevante normen zoals:
    a) NPR 5313 - Computerruimtes en datacenters - Beveiliging
    b) NTA 8012 - Beperking van schade als gevolg van brand van en via de elektrische leidingen in de elektrische installatie
    c) NTA 8073 - Vaste brandblusinstallaties - Automatische sprinklerinstallaties
    d) NEN-EN-ISO 20957 - Vast opgestelde trainingsapparatuur - Veiligheidseisen en beproevingsmethoden.
    e) Centrum voor Criminaliteitspreventie en Veiligheid (CCV), VRKI - Richtlijn inbraakbeveiliging onderwijsinstellingen versie 1.4 maart 2014
218. Zijn ontruimingsplannen voor alle gebouwen actueel en geoefend?
219. Wordt bij het ontwerp, de bouw en de inrichting van gebouwen rekening gehouden met onder andere inbraak, insluiping, diefstal, ongewenst gedrag en met brand?
220. Wordt bij het ontwerp, de bouw en de inrichting van gebouwen rekening gehouden met onder andere sociale veiligheid en informatieveiligheid?
221. Wordt toegangsbeheersing, compartimentering en ontruiming van een gebouw beoordeeld vanuit verschillende veiligheidsthema's, zoals brandveiligheid, inbraakpreventie, inbraakwerendheid, sociale veiligheid en informatieveiligheid?
222. Vindt regelmatig instructie en oefening van gebruikers van de gebouwen, waaronder de aangewezen BHV'ers plaats?

8.11 Crisismanagement, BHV, BCM

223. Heeft uw instelling een coördinator op crisismanagement, BHV en BCM?
224. Is crisismanagement, BHV en BCM belegd in één van de portefeuilles van het College van Bestuur?
225. Is binnen uw instelling voldoende kennis aanwezig op crisismanagement, BHV en BCM?
226. Heeft uw instelling een beleid op crisismanagement, BHV en BCM?
227. Kan uw instelling zich verantwoorden op een gepaste omgang met crisismanagement, BHV, BCM?
228. Is uw instelling voldoende op een crisis voorbereid?
229. Zijn taken en verantwoordelijkheden voor in een crisis situatie al toebedeeld?
230. Weet een ieder wat er van hem of haar wordt verwacht?
231. Zijn adequate hulpmiddelen voor handen?
232. Is men geïnformeerd, geoefend en bekwaam?
233. Hanteert uw instelling oefenplannen en –cycli om crisismanagement te verbeteren?
234. Hanteert uw instelling NEN-ISO 22301 - Managementsystemen voor bedrijfscontinuïteit – Eisen?
235. Hanteert uw instelling NEN-ISO 22313 - Business continuity managementsystemen – Leidraad?

Check

9 Evaluatie van de werking

9.1 Bewaking, meting, analyse en evaluatie

236. Is er bepaald wat moet worden bewaakt en gemeten?
237. Zijn de methodes voor bewaken, meten, analyseren en evalueren om geldige resultaten te bereiken bepaald?
238. Is er bepaald wanneer moet worden bewaakt en gemeten?
239. Is er bepaald wanneer de resultaten van bewaking en meting moeten worden geanalyseerd en beoordeeld?
240. Zijn de relevante gedocumenteerde informatie bewaart als bewijs van de resultaten?
241. Is de uitvoering van MIVH beoordeeld?
242. Is de effectiviteit van MIVH beoordeeld?

9.2 Interne audits

243. Met geplande tussenpozen worden interne audits uitgevoerd?
244. Leveren die audits informatie of wordt geconformeerd aan de eisen die de instelling heeft gesteld aan het MIVH?
245. Leveren die audits informatie of wordt geconformeerd aan de eisen die volgen uit deze norm?
246. Leveren die audits informatie of MIVH effectief is geïmplementeerd en onderhouden?
247. Er is/zijn één of meer auditprogramma's gepland, vastgesteld, geïmplementeerd en onderhouden, met inbegrip van methoden, verantwoordelijkheden, planningseisen en rapportage.
248. Is hierbij het belang van de betreffende processen en de uitkomsten van voorafgaande audits hierin betrokken?

249. Zijn de auditcriteria en het bereik van elke audit bepaald?
250. Zijn auditors geselecteerd en de objectiviteit en onpartijdigheid van het auditproces bewaakt?
251. Zijn/worden de auditresultaten gerapporteerd aan het relevante management?
252. Wordt de gedocumenteerde informatie bewaard als bewijs van het audit-programma en de auditresultaten?

9.3 Management review

253. Heeft de hoogste leiding met geplande tussenpozen het MIVH beoordeeld en daarbij telkens de voortdurende geschiktheid, toereikendheid en effectiviteit vastgesteld?
254. Is in de management review de status van acties naar aanleiding van vorige management reviews betrokken?
255. Zijn in de management review wijzigingen in ex- en interne aangelegenheden betrokken, die van belang voor MIVH?
256. Is de management review informatie over de uitvoering van MIVH betrokken, waaronder ontwikkelingen omtrent non-conformiteiten en correctieve acties, bewakings- en metingsresultaten en auditresultaten?
257. Zijn in de management review mogelijkheden voor continue verbeteringen betrokken?
258. Omvatten de uitkomsten van een management review beslissingen ten aanzien van continue verbetering van MIVH?
259. Omvatten de uitkomsten van een management review de noodzaak voor eventuele wijzigingen van MIVH?
260. Wordt gedocumenteerde informatie als bewijs voor de uitkomsten van management reviews bewaard?

Act

10 Verbetering

10.1 Non-conformiteiten en corrigerende acties

261. Is bij elke non-conformiteit die zich voordeed gereageerd op de non-conformiteit?
262. Is daarbij tevens actie ondernomen om het te beheersen en corrigeren?
263. Zijn ook de gevolgen afgehandeld?
264. Is bij elke non-conformiteit die zich voordeed de noodzaak van acties beoordeeld voor het elimineren van de oorzaken van de non-conformiteit, door de non-conformiteit te beoordelen, de oorzaken van de non-conformiteit vast te stellen en vast te stellen of zich vergelijkbare non-conformiteiten voordoen of mogelijk kunnen optreden?
265. Zijn bij elke non-conformiteit die zich voordeed de nodige acties geïmplementeerd?
266. Is bij elke non-conformiteit die zich voordeed de effectiviteit van elke corrigerende activiteit beoordeeld?
267. Is bij elke non-conformiteit die zich voordeed indien nodig wijzigingen in MIVH aangebracht?
268. Waren de corrigerende acties in overeenstemming met de non-conformiteit die ontstond?
269. Wordt gedocumenteerde informatie bewaard als bewijs van de aard van de non-conformiteiten en de acties die naar aanleiding daarvan zijn genomen, alsmede de resultaten van de corrigerende acties?

10.2 Voortdurende verbetering

270. Wordt de geschiktheid van MIVH voortdurend verbeterd?
271. Wordt de toereikendheid van MIVH voortdurend verbeterd?
272. Wordt de effectiviteit van MIVH voortdurend verbeterd?

Colofon

Opdrachtgever:	Projectgroep Integrale Veiligheid Hoger Onderwijs
Projectcontact:	Paul Goossens (p.a.m.goossens@hr.nl)
Opgesteld door:	Joris Hutter en Marcel Spit (Adviescentrum BVI)
Bijdragen van:	Jeroen Terstegge (Privacy Management Partners) Alex Ivanovic (Adviesbureau Forta Nova)

Over Integraal Veilig Hoger Onderwijs

Het ministerie van OCW, een aantal hogescholen en universiteiten en kenniscentra hebben de handen ineen geslagen en een platform gecreëerd voor bundeling van kennis over en ervaring in integrale veiligheid in het hoger onderwijs. Het platform werkt gefaseerd aan het verzamelen en ontwikkelen van instrumenten op het gebied van Integrale Veiligheid.

Deze uitgave maakt onderdeel uit van de ontwikkelde instrumenten voor het hogeronderwijs. Alle producten zijn kosteloos voor de onderwijsinstellingen beschikbaar gesteld op de website. Naast de eigen ontwikkelde instrumenten delen onderwijsinstellingen ook good practices en ervaringen, hiermee versterken de instellingen gezamenlijk de veiligheid in het hoger onderwijs.

INTEGRALE
VEILIGHEID
HOGER ONDERWIJS

http://www.integraalveilig-ho.nl