



Referentiekader: de inrichting en governance van Integrale Veiligheid



PLATFORM
INTEGRALE VEILIGHEID
HOGER ONDERWIJS

Een initiatief van de Vereniging Hogescholen en UNL



Referentiekader: de inrichting en governance van Integrale Veiligheid

Inleiding

Dit door KPMG opgestelde referentiekader Integrale Veiligheid beoogt bestuurders in het Hoger Onderwijs en hun stafdiensten te ondersteunen bij het effectief inrichten en waarborgen van de governance van Integrale Veiligheid in de gehele instelling. Deze notitie belicht expliciet de cruciale rollen van Manager Integrale Veiligheid, CISO en adviseur Kennisveiligheid binnen HO-instellingen. Tevens treft u praktische richtlijnen aan voor het verbinden van risicomanagement aan het veelgebruikte drie-lijnsmodel¹ en de positionering van de Manager Integrale Veiligheid hierin. Dit referentiekader is opgesteld in opdracht van het subsidieprogramma Platform IV-HO en vormt een vervolg op twee eerdere expertnotities².

Huidige en toekomstige uitdagingen in Integrale Veiligheid

In recente jaren hebben verschillende incidenten, waaronder ransomware-aanvallen, interventies door staatelijke actoren, radicalisering onder studenten, inbreuken op wetenschappelijke integriteit en onveilige werkomgevingen, overtuigend het belang aangetoond van een veiligheidsbeleid dat risicogericht is en niet louter compliance-gericht. Dergelijke voorvallen onderstrepen de noodzaak voor bestuurders om over proactieve risicobeheerstrategieën te beschikken.

Integrale Veiligheid is een dynamisch en continu evoluerend vakgebied, gericht op het beheren van de toenemende complexiteit van veiligheidskwesties in een veranderende wereld. Stol et al. (2016) beschrijven Integrale Veiligheid als een benadering om complexe veiligheidsproblemen te beheersen. Daarbij zijn samenhang en coördinatie tussen de veiligheidsthema's essentieel. Deze thema's betreffen onder andere internationalisering, cyberveiligheid, privacy, sociale veiligheid, integriteit, kennisveiligheid & ongewenste beïnvloeding, gebouwveiligheid beveiliging & BHV, zorgwekkend gedrag & radicalisering, arbo & milieu. Door geopolitieke en maatschappelijke ontwikkelingen zijn deze thema's geen statisch geheel, er kunnen nieuwe aandachtsgebieden ontstaan. Verder kan de organisatorische inrichting van deze thema's verschillen vanwege hun oorsprong, aard en volwassenheidsniveau. Het naar elkaar toegroeien en het systematisch en risicogericht benaderen van de thema's versterkt de veiligheid in en van een instelling.

Integrale Veiligheid streeft naar het minimaliseren van gevaren en verstoringen binnen de leer- en werkomgeving. Dit wordt bereikt door een risicomanagementcyclus die risico's identificeert en, afhankelijk van de situatie, expliciet accepteert of mitigeert. Deze methodische aanpak faciliteert het maken van strategische beslissingen over welke risico's moeten worden gereduceerd of geheel geëlimineerd en welke risico's aanvaard worden.

Aangezien Integrale Veiligheid meerdere thema's omvat, vereist het een collectieve inspanning van diverse organisatieonderdelen en personen. Dit continue proces zorgt ervoor dat HO-instellingen zowel in control zijn en wendbaar en weerbaar blijven, opdat zij adequaat kunnen reageren op veranderende omstandigheden. Veel instellingen ervaren echter uitdagingen bij het invoeren en institutionaliseren van een risicogestuurde

¹ www.iaa.nl/actualiteit/nieuws/belangrijke-update-three-lines-model

² Expertnotitie IV-HO en KPMG 'Cybersecurity Pas Toe of Leg Uit' en de 'Handreiking Governance van Privacy'

benadering, waardoor het eigenaarschap van risico's onvoldoende verankerd raakt en functionarissen die risico-eigenaren zouden moeten bijstaan, vaak niet doeltreffend gepositioneerd zijn³. Dit is recent benadrukt door de minister van OCW, die wijst op het belang van risicobeheersing inzake Kennisveiligheid, als onderdeel van de bestuurlijke afspraak om de Nationale Leidraad Kennisveiligheid te implementeren⁴.

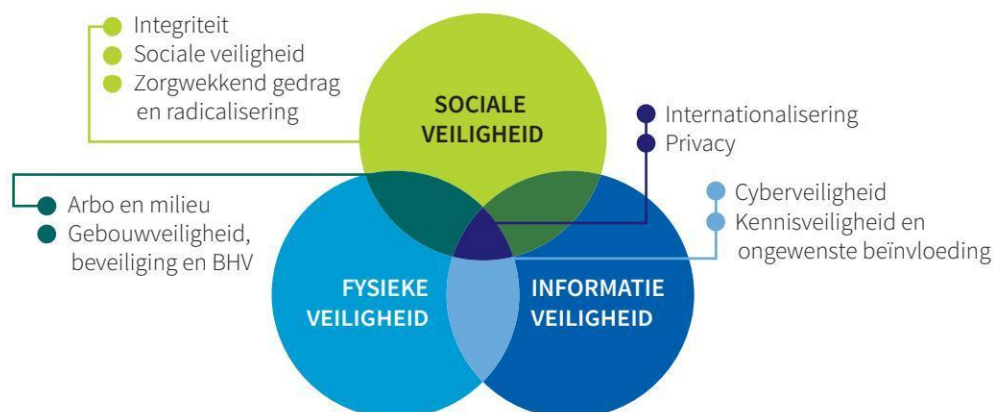
Integrale Veiligheid als dynamische discipline

Integrale Veiligheid is complex en veelzijdig. Door de intensieve samenwerking in onderwijs en onderzoek is het belangrijk dat alle betrokkenen een uniforme invulling geven aan dit begrip. Dit is des te belangrijker vanwege het bestaan van bestuurlijke afspraken over het toepassen van risicomanagement. Hierbij wordt echter veel ruimte gelaten voor zelfregulering⁵. Het is van belang deze zelfregulering duidelijk te maken aan politiek en regelgevers.

In het HO wordt Integrale Veiligheid gedefinieerd als een PDCA-cyclus die bestaat uit vijf samenhangende processen:

1. Het verwerven van sturingsinformatie over kansen en risico's;
2. Het ontwikkelen van veiligheidsbeleid en risicobeheerprocessen;
3. Het vaststellen van taken, rollen en verantwoordelijkheden voor veiligheid in de organisatie;
4. Het bevorderen van bewustzijn over de verwachtingen bij te dragen aan de veiligheidscultuur;
5. Continuïteitsmanagement: de benaderingen voor het omgaan met incidenten, calamiteiten of crises om de voortgang van de kernprocessen te waarborgen en de reputatie te beschermen.

Deze vijf coördinerende processen zijn generiek voor de tien veiligheidsthema's die sinds de introductie in 2012 door het HO worden gehanteerd. Voor overzichtelijkheid worden de veiligheidsthema's in onderstaande drie domeinen geplaatst.



Codes Goed Bestuur

De codes Goed Bestuur van zowel de Vereniging van Hogescholen (VH) als Universiteiten van Nederland (UNL) behelsden tot voor kort een statement dat de instelling beschikt over professionele interne risicobeheersings- en controlesystemen⁶. In de meest recente VH-versie is deze term gewijzigd in 'kwaliteitsmanagement', risicomanagement is onderdeel daarvan.

³ [Cyberdreigingsbeeld 2023 \(surf.nl\)](#)

⁴ [Kamerbrief 16 oktober 2023 bij Sectorbeeld kennisveiligheid universiteiten | Kamerstuk | Rijksoverheid.nl](#)

⁵ Rotterdamverklaring, Intentieverklaring Integrale Veiligheid Hoger Onderwijs, Bestuursakkoord 2022, de Nationale Leidraad Kennisveiligheid en de branchecodes in het HO

⁶ [Branchecode Goed bestuur en toezicht in het hbo en Code goed bestuur universiteiten](#)

Integrale Veiligheid en de dynamiek in risicobeheersing

Door strategische doelen te benaderen vanuit kansen en risico's, ontwikkelen HO-instellingen een veiligheids-perspectief dat traditionele methoden overstijgt. Dit leidt tot een proactieve aanpak, waarbij uitdagingen worden aangegaan, kansen benut en risico's effectief gemanaged worden. En niet louter operationele risico's, ook strategische. Hierdoor worden kernwaarden, kroonjuwelen en primaire processen beschermd en ontstaat ruimte voor innovatie in onderwijs en onderzoek.

De principes van risicomanagement zijn al grotendeels geïmplementeerd in gebieden zoals financiën, informatiebeveiliging en arbeidsomstandigheden via een periodieke risico-inventarisatie en -evaluatiecyclus. Voor sociale veiligheid wordt van instellingen verwacht dat zij risicoprofielen opstellen, zoals bepleit door regeringscommissaris Hamer. In het kennisveiligheidsbeleid van OCW is zelfregulering eveneens de norm⁷.



JAN LINTSEN (LID CVB VAN DE UNIVERSITEIT VAN AMSTERDAM):

**“HOUD RISICOMANAGEMENT
OP STRATEGISCH NIVEAU, ZODAT HET CVB
KEUZEMOGELIJKHEDEN KAN AFWEGEN,
ANDERS WORDT HET TE MECHANISCH
EN BUREAUCRATISCH EN HEEFT HET
ONVOLDOENDE NUT”.**

IV-HO Framework voor Integrale Veiligheid

De door IV-HO ontwikkelde methodiek⁸ helpt bestuurders en Integrale Veiligheidsmedewerkers om de veiligheidsthema's in hun instelling in te richten. De principes gelden zowel voor grote als kleine instellingen. In dit laatste geval zijn er minder (staf)medewerkers en zijn niet-conflicterende veiligheidsrollen in één functie (en persoon) verenigd. Een risicogerichte aanpak leidt tot proportionele maatregelen zodat risico's tot een acceptabel niveau zijn teruggebracht. Door het inzichtelijk maken van risico's kunnen er bewuste keuzes gemaakt worden over wat er wel of juist niet (aan) gedaan moet worden.

Om overzicht van de risico's te creëren is het belangrijk dat Integrale Veiligheid verder wordt geprofessionaliseerd, onder andere door het gebruik van instrumenten zoals risicoanalyses, begrotingen, meerjarenplanning, reviews/audits, e.d. De Manager Integrale Veiligheid kan door het toepassen van deze instrumenten een strategische beleids- en adviesfunctie voor het bestuur vervullen. Integrale Veiligheid zal als bedrijfsfunctie moeten groeien van functioneel gescheiden silo's naar het integraal monitoren en beheersen van veiligheid. Hierbij worden vijf ontwikkelfasen onderscheiden:

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

⁷ Uiteengezet in hoofdstuk 6 van de [Nationale Leidraad Kennisveiligheid](#)

⁸ Zie animatie over het [IV-HO framework Integrale Veiligheid](#)

In dit groeimodel⁹, gebaseerd op de 'safety culture ladder', bouwt elke volgende stap voort op wat is bereikt in de voorgaande. Echter, voor elke instelling kan een ander niveau toereikend zijn.

Kritieke succesfactoren bij de inrichting van Integrale Veiligheid

Twee hoofdfactoren dragen bij aan de acceptatie en effectiviteit van de inspanningen op veiligheidsgebied: de positionering en de competenties van de 2^e-lijnsfunctionarissen. Voor een effectieve inrichting dient de HO-instelling de competente personen op de juiste plaatsen te positioneren, opdat zij het bestuur optimaal kunnen ondersteunen en adviseren.

Wij hebben navolgend drie specifieke rollen uitgelicht, de Manager Integrale Veiligheid, de CISO en de adviseur Kennisveiligheid. Hiervoor is gekozen omdat de Manager de centrale 'aanvoerder' is voor alle veiligheids-thema's, de CISO vanwege diens ontworteling van de IT-organisatie en de adviseur Kennisveiligheid vanwege de recente ontwikkeling van dit thema.

Manager Integrale Veiligheid: strategisch adviseur en spin in het web

De wijze waarop een Manager Integrale Veiligheid in een organisatie gepositioneerd is reflecteert de prioriteit die de instelling aan dit onderwerp geeft. Voor het verhogen van veiligheidsbewustzijn en het creëren van draagvlak dient het CvB betrokken te zijn bij het veiligheidsbeleid. Wij raden aan dat de Manager Integrale Veiligheid een directe communicatielijn heeft met het CvB, en naar diens inzicht en in specifieke omstandigheden, ook met de Raad van Toezicht (RvT). Deze functie moet in staat zijn om strategische risico's en belangrijke beleids- en organisatievoorstellen rechtstreeks aan het bestuur voor te leggen, onafhankelijk van een direct leidinggevende. De Raad van Toezicht wordt periodiek, minimaal halfjaarlijks bijgepraat over veiligheidsonderwerpen en de meerjarenstrategie voor Integrale Veiligheid.

De Manager Integrale Veiligheid opereert als primus inter pares voor alle veiligheidsfuncties en gedraagt zich als generalist om in samenhang en strategisch over het gehele werkveld te kunnen adviseren. Deze Manager coördineert de diverse veiligheidsactiviteiten, maar stuurt nadrukkelijk niet de andere veiligheidsfuncties aan.

De Manager, de CISO en adviseurs op de verschillende veiligheidsthema's zijn ondergebracht in de 2^e-lijn. Een uitzondering hierop is de Functionaris Gegevensbescherming (FG), die als wettelijk gedelegeerd toezichthouder in de 3^e-lijn functioneert.

Grotere instellingen hebben vaak een onafhankelijke Interne Auditfunctie in de derde lijn, die niet alleen de veiligheidsprocessen en -maatregelen toetst, maar ook de effectiviteit van de governance en samenwerking. Onderwijsinstellingen die niet over interne auditors beschikken kunnen zich extern laten evalueren, bijvoorbeeld op verzoek van het CvB of onafhankelijk in opdracht van de RvT. Voor informatiebeveiliging is externe toetsing al gebruikelijk via periodieke SURFaudits inzake informatiebeveiliging of via IT-audits in het kader van de jaarrekeningcontrole; voor andere veiligheidsthema's is dit minder of niet georganiseerd, waardoor het CvB beperkte sturingsinformatie ontvangt om strategische risico's te wegen ten opzichte van de organisatie-doelen.

Dezelfde principes gelden voor alle veiligheidsthema's. Het is van belang dat er voor elk thema verantwoordelijken zijn toegewezen en dat er integratie plaatsvindt via coördinerende processen. Dit zorgt voor een centraal overzicht en samenhang, vaak ondersteund door een strategisch overleg(orgaan) voor periodieke en multidisciplinaire risicoafweging en gecoördineerde activiteiten. Daarnaast moet de Manager Integrale Veiligheid en het veiligheidsnetwerk binnen de instelling vroegtijdig betrokken worden bij ontwikkelingen, projecten of nieuwe initiatieven, zodat alle veiligheidsthema's voldoende aandacht krijgen, ongeacht fluctuerende prioriteiten door actuele ontwikkelingen en korte termijndeadlines.

⁹ Toolkit implementatie framework Integrale Veiligheid Hoger Onderwijs

Op thema's die al verder ontwikkeld zijn, zoals ARBO, fysieke beveiliging en BHV, raden wij positionering binnen een beleidsdirectie of in de lijn te worden overwogen, onder de voorwaarde dat de functionele verbinding met de Manager Integrale Veiligheid gehandhaafd blijft. Tenslotte heeft het voor een sectorbreed begrip en toepassing de voorkeur om deze veiligheidsfuncties op te nemen in de functiehuizen in het HO.



JOEP HOUTERMAN (LID CVB FONTYS):

**“SYSTEMATISCH AANDACHT GEVEN EN
EROVER RAPPORTEREN IS ONMISBAAR
VOOR HET STERK VERBETEREN VAN
DE INTEGRALE VEILIGHEID”.**

Chief Information Security Officer

Net als de Manager Integrale Veiligheid en de adviseur Kennisveiligheid, is de functie van Chief Information Security Officer (CISO) het meest effectief wanneer deze kan optreden als bestuurlijk adviseur. Een onafhankelijke positionering van de CISO buiten de ICT- en IM-verantwoordelijke draagt bij aan een effectieve governance in de instelling. De CISO is voornamelijk een 2^e-lijnsfunctie: de gemandateerde beleidsmaker, cyberrisicomanager en expertmatig adviseur van het bestuur en de 1^e lijn. Wel dient de 3^e-lijnsfunctie van security monitoring ingevuld te zijn, zoals bij privacy met een Chief Privacy Officer als beleids- en adviesfunctie in de 2^e lijn en een FG als interne toezichthouder in de 3^e lijn.

Daarnaast dient de CISO, net als de Manager Integrale Veiligheid over een toereikend mandaat en eigen budget te beschikken. Deze combinatie stelt de CISO in staat om beleid en richtlijnen uit te vaardigen, prioriteiten te bepalen, een intern netwerk van beveiligingsrollen te realiseren, eigen initiatieven te ontplooiën e.d. Hierdoor kan de CISO volwaardig en krachtig functioneren.

Onderzoek in het HO heeft aangetoond dat een hogere betrokkenheid van bestuurders direct correleert met betere resultaten op het gebied van informatieveiligheid¹⁰ en minder incidenten. Een onafhankelijke positie van de CISO is dan ook fundamenteel om een adequaat intern tegenwicht te bieden en essentiële ‘checks & balances’ te garanderen. Dit maakt het voor de CISO mogelijk om het CvB onafhankelijk en proactief te adviseren, zelfs wanneer dit advies mogelijk tegenstrijdig is met de visie of prioriteiten van lijn- of IT/IM-verantwoordelijken. Zonder deze onafhankelijkheid mist de organisatie een tegenkracht bij interne belangen- tegenstellingen.

Adviseur Kennisveiligheid

Het functiegebied Kennisveiligheid is met name bij (technische) universiteiten door geopolitieke ontwikkelingen de laatste jaren sterk in belang gestegen. Kleinere instellingen stellen geen specifieke themafunctionaris hiervoor aan, maar beleggen dit in de lijn en verdelen deze verantwoordelijkheid over een of meerdere andere functionarissen, zoals de Manager Integrale Veiligheid of de CISO, vaak binnen een intern samenwerkingsverband of overlegorgaan. Wij raden een centrale positionering van de adviseur Kennisveiligheid aan, plaatsing binnen het staf- of bestuursbureau, dichtbij het CvB, de CISO en de Manager Integrale Veiligheid.

¹⁰ Governance-onderzoek: betrokkenheid bestuurders komt ten goede aan informatieveiligheid - MBO Digitaal

Andere functionarissen betrokken bij Integrale Veiligheid

Voor thema's zoals sociale veiligheid, ARBO en andere veiligheidsaspecten zijn in de meeste grote instellingen functionarissen aangesteld binnen beleidsdirecties of uitvoerende diensten, zoals vertrouwenspersonen en ombudsfunctionarissen bij HRM en adviseurs Fysieke en Gebouwbeveiliging bij Facilities. Waar mogelijk raden wij een onafhankelijke positionering van deze veiligheidsfuncties aan. Dit kan in een afdeling Integrale Veiligheid of GRC, waar onder leiding van de Manager zich ook de bovengenoemde functies bevinden. Waar dit niet mogelijk is dienen er voldoende waarborgen voor hun onafhankelijkheid en voor een sterke verbinding met de andere veiligheidsfuncties aanwezig te zijn. Dit voorkomt nieuwe afhankelijkheden en zorgt ervoor dat de Manager Integrale Veiligheid, in samenwerking met de CISO en andere strategische veiligheidsadviseurs, onafhankelijk kan opereren en zonder interne politieke druk het CvB kan adviseren.

Competenties van sleutelfuncties in Integrale Veiligheid

Functies zoals de Manager Integrale Veiligheid, CISO, Chief Privacy Officer en adviseur Kennisveiligheid vereisen een aantal kerncompetenties, deze omvatten:

- Strategisch adviseur: Deze rol vereist de bekwaamheid om strategisch advies te geven dat de richting van de organisatie kan beïnvloeden;
- Risicomanager: Het vermogen om risico's te identificeren, te beoordelen en te managen;
- Beleidsmedewerker: Het ontwikkelen, implementeren en handhaven van beleid dat veiligheidsnormen ondersteunt;
- Verbinder: Het vermogen om verschillende partijen binnen en buiten de organisatie samen te brengen;
- Aanjager: Het stimuleren van naleving en bevordering van veiligheidsbewustzijn;
- Crisismanager: Het beheren van noodsituaties, van voorbereiding tot reactie en nazorg.

Specifieke rollen en verantwoordelijkheden

- De Manager Integrale Veiligheid staat centraal in de bescherming en waarborging van de veiligheid binnen instellingen. Deze rol vereist een grondig begrip van diverse veiligheidsthema's en de samenhang ertussen. Deze Manager brengt relevante partijen samen, verkoopt' veiligheid intern en stimuleert de naleving van veiligheidsmaatregelen;
- De CISO en de adviseur Kennisveiligheid zijn primair strategische adviseurs en sparringpartners van het CvB voor hun vakgebieden. De CISO richt zich op informatiebeveiliging, terwijl de Adviseur Kennisveiligheid zich bezighoudt met het voorkomen van ongewenste kennisoverdracht of van de beïnvloeding van onderwijs en onderzoek door externe actoren;
- De FG heeft een interne toezichthoudende functie.

Een kenmerkende eigenschap van veiligheidsfunctionarissen is hun onafhankelijkheid, wat hem of haar in staat stelt om objectief te adviseren zonder beïnvloeding van een leidinggevende of het bestuur. Dit omvat tevens een directe rapportagelijijn naar het CvB en indien nodig naar de auditcommissie of RvT bij grote veiligheidsincidenten of aanhoudende kwetsbaarheden.

De Manager Integrale Veiligheid en andere genoemde veiligheidsfuncties dragen nadrukkelijk geen directe verantwoordelijkheid voor de implementatie van adviezen of maatregelen; deze verantwoordelijkheid ligt bij de lijnorganisatie. Niettemin zijn de zichtbaarheid en directe toegankelijkheid van de Manager Integrale Veiligheid noodzakelijk voor het effectieve informeren en ondersteunen van het bestuur bij het nemen van onderbouwde beslissingen en het realiseren ervan. De combinatie van deskundigheid, onafhankelijkheid en verbindend en inspirerend leiderschap versterkt de positie van de Manager Integrale Veiligheid als sleutelfiguur binnen de instelling. Het erkennen en faciliteren van deze rol door CvB, RvT en MR is van belang voor het creëren van een veilige en veerkrachtige onderwijs- en onderzoeksomgeving.

Conclusie: welke stappen leiden tot succesvolle governancestructuur voor Integrale Veiligheid?

Voor de HO-instelling leiden de volgende stappen tot een succesvol ingerichte governance van Integrale Veiligheid. Zoals eerder benoemd bestaat er geen generieke oplossing die voor iedere instelling en situatie geschikt is; het is maatwerk. Echter, de volgende adviezen bieden handvatten voor een effectieve inrichting:

- **Integratie veiligheidsthema's:** Verbind alle veiligheidsthema's onderling, uitgaande van de principes van risicomanagement. Een brede en samenhangende benadering, waarbij alle veiligheidsthema's gezamenlijk worden gecoördineerd en beheerd, is onontbeerlijk voor een coherente aanpak van Integrale Veiligheid.
- **Toewijzing verantwoordelijkheden/eigenaarschap:** Wijs de verschillende veiligheidsthema's eenduidig toe aan specifieke verantwoordelijken. Deze functies moeten formeel onafhankelijk kunnen opereren en over een directe communicatielijn met het College van Bestuur beschikken. Daarnaast moet het eigenaarschap van specifieke risico's in de 1^e lijn worden belegd bij de proceseigenaren, directeuren, leidinggevers en docenten, zodat zij hun doelstellingen effectief kunnen halen en risico's goed kunnen beheersen. Wij raden aan de functieomschrijvingen en -benamingen zoveel mogelijk overeenkomstig te maken voor de verschillende veiligheidsfuncties.
- **Positionering van Integrale Veiligheid:** Plaats de functionarissen voor Integrale Veiligheid, zoals de Manager, CISO, FG en andere veiligheidsfuncties op een onafhankelijke positie zodat zij zonder last en ruggenspraak kunnen opereren en het bestuur kunnen adviseren. Dit waarborgt de integriteit van de instelling. Het is van belang dat deze functionarissen in een 2^e-lijnsfunctie opereren (met de FG als 3^e-lijnsfunctie), zodat zij onafhankelijk en objectief hun werkzaamheden kunnen verrichten. Dit kan het beste in een afzonderlijke stafafdeling, bij kleinere instellingen eventueel verspreid over functionele afdelingen – mits voorzien van voldoende aanvullende waarborgen.
- **Mandaat & budget:** Garandeer dat de Manager Integrale Veiligheid, de CISO en functionarissen voor de andere thema's over een expliciet mandaat en toereikend budget beschikken. Hun rol binnen de instelling moet voldoende gewicht hebben om effectief te kunnen opereren en een onafhankelijke adviesrol te kunnen vervullen.
- **Oprichting intern platform Integrale Veiligheid:** Richt een integraal veiligheidsplatform in, bestaande uit leden met specifieke verantwoordelijkheden voor de diverse veiligheidsthema's. Dit platform of overlegorgaan overziet de kernrisico's, adviseert het bestuur, en waarborgt de uitvoering van veiligheidsstrategieën en -maatregelen, en beleidsmatige ontwikkelingen. Waar nodig worden in decentrale organisatieonderdelen de veiligheidsfuncties ook gebundeld in decentrale platforms die de lijnverantwoordelijkheid met raad en daad ondersteunen.
- **Regelmatig overleg en meerjarenplan (PDCA-cyclus):** Organiseer op regelmatige basis, minimaal halfjaarlijks gestructureerd overleg op strategisch niveau over Integrale Veiligheid. Deze sessies zijn bedoeld voor het bespreken van strategische risico's en belangrijke actuele kwesties, voor het ontwikkelen van meerjaren- en actieplannen en voor het evalueren van de voortgang van geïmplementeerde beheersmaatregelen en van de effectiviteit van de veiligheidsorganisatie. Wij raden ook jaarlijkse rapportage over Integrale Veiligheid aan CvB, RvT en andere belanghebbenden aan, bij voorkeur geïntegreerd in de planning- en controlcyclus.
- **In/externe audit:** Koppel de interne auditfunctie aan de werking van het beoogde interne risicobeheersingssysteem. De scope van het huidige SURFaudit toetsingskader voor Informatiebeveiliging kan worden vergezeld van toetsingskaders inzake andere veiligheidsthema's om behulpzaam te zijn bij het risicogericht verbeteren van de veiligheidsprocessen, bij self-assessments of bij periodieke toetsingen. Beperk de auditlast door op roulerende wijze de veiligheidsthema's aan een toetsing te onderwerpen.

- **Samenwerking in de keten:** verbreed de samenwerking in de (HO- en veiligheids)ketens en stimuleer sectorbrede initiatieven, zoals het delen van risico-informatie, beleidsstukken, richtlijnen en documenten, het inkopen van producten of diensten, het uitwisselen van kennis en personeel of zelfs het gezamenlijk aanstellen van veiligheidsfunctionarissen en het op bestuurlijk niveau bespreken van dilemma's bij het afwegen van kansen en risico's.
- **Actieve samenwerking met in/externe toezichthouders:** Onderhoud een sterke en transparante relatie met zowel interne als externe toezichthouders. Deze samenwerking moet gericht zijn op een open dialoog met partijen zoals de RvT, interne auditors, accountant, Inspectie van het Onderwijs en Autoriteit Persoonsgegevens. Dit bevordert de naleving van wet- en regelgeving, ondersteunt een cultuur van verantwoordelijkheid, en biedt inzichten die cruciaal zijn voor het verfijnen van risicomanagement en Integrale Veiligheid. Actieve communicatie en transparante verantwoording over beleid en veiligheidsniveau(s) versterkt de geloofwaardigheid bij toezichthouders en andere belanghebbenden.
- **Kennisvergroting:** Wij raden aan om MR- en RvT-leden, bestuurders, decanen en directeuren bij te scholen op het gebied van risicomanagement en de veiligheidsthema's, met aandacht voor een integrale aanpak. Gebruik hierbij middelen zoals de e-learning 'IV voor Medezeggenschap'¹¹, zoals ontwikkeld door Platform IV-HO, om deze scholing te ondersteunen. Verder kunnen binnen Integrale Veiligheid de jongere vakgebieden leren van de reeds volwassen opererende veiligheidsfuncties.



¹¹ E-learning: [Medezeggenschap & Integrale Veiligheid](#)