Deloitte.

Verkennend onderzoek naar de toepasbaarheid van een volwassenheidsmodel op het gebied van kennisveiligheid bij kennisinstellingen

Mei 2024

Inhoud

Managementsamenvatting

Achtergrond en Doelstelling

Deze voorverkenning, geïnitieerd door het ministerie van Onderwijs, Cultuur en Wetenschap (OCW), onderzoekt de toegevoegde waarde, mogelijkheden en toepasbaarheid van een volwassenheidsmodel voor kennisveiligheid binnen kennisinstellingen in het hoger onderwijs. Deze inspanning is onderdeel van een breder streven om de weerbaarheid van deze instellingen te versterken in het licht van internationale samenwerking en de daarmee gepaard gaande risico's zoals ongewenste kennisoverdracht, heimelijke beïnvloeding en ethische kwesties.

Belangrijkste Bevindingen

Een volwassenheidsmodel kan aanzienlijke voordelen bieden voor de verbetering van kennisveiligheid door een duidelijk raamwerk voor procesevaluatie en verbetering te bieden.

- Met het oog op de waarborging van de nationale veiligheid heeft OCW behoefte aan inzicht in de verschillen en de mate van ontwikkeling van de sector op het gebied van kennisveiligheid. Dit inzicht is cruciaal om het kennisveiligheidsbeleid verder te ontwikkelen, het prioriteren van acties en het alloceren van middelen om de weerbaarheid van de sector als geheel te vergroten.
- Deloitte is van mening dat de toepassing van een volwassenheidsmodel organisaties kan helpen strategische prioriteiten te stellen en duidelijkheid te scheppen over verantwoordelijkheden.
- Bij kennisinstellingen bestaan echter zorgen over de diversiteit in risicoprofielen en de mogelijke verwaarlozing van niet-meetbare aspecten zoals organisatiecultuur en leervermogen. Er is bij kennisinstellingen consensus dat een uniform volwassenheidsmodel, ondanks het potentieel, vooral ervaren wordt als een controlemiddel en dat het bij toepassing vooral gebruikt zou moeten worden als leermiddel. Daarbij uiten zij de behoefte aan een sterkere rol voor OCW in het bieden van duidelijke (risicomanagement)richtlijnen en praktische ondersteuning, in combinatie met de bevordering van samenwerking met Europese partners.

Aanbevelingen Deloitte

Zoek de verbinding met kennisinstellingen en koepels en onderzoek de kansen van (door)ontwikkeling van reeds bestaande (opzetten van) volwassenheidsmodellen. Door een volwassenheidsmodel flexibel en aanpasbaar te maken kan het aansluiten bij de diverse behoeften en risicoprofielen binnen het onderwijs- en onderzoekslandschap als ook die van OCW op het gebied van nationale veiligheid. Focus daarbij in eerste instantie op continue verbetering en ontwikkeling, en minder op strikte naleving van compliance-normen. Biedt hiervoor de door kennisinstellingen gevraagde support: zowel in duidelijkheid over rollen en verantwoordelijkheden van overheid en instellingen als ook in de ontwikkeling van ondersteunende tools die passen bij de Nederlandse context.

Conclusie

Een volwassenheidsmodel voor kennisveiligheid kan een bijdrage leveren aan het versterken van de weerbaarheid van kennisinstellingen, mits de implementatie ervan rekening houdt met de uniciteit van elke instelling en de risico's eigen aan de sector. Dit vraagt om samenwerking tussen OCW, koepels en kennisinstellingen, met een nadruk op wederzijds begrip van belangen, communicatie en een cultuur van continue verbetering.

1. Introductie

In deze voorverkenning wordt onderzocht wat de mogelijke toegevoegde waarde is van de toepassing van een volwassenheidsmodel op het gebied van kennisveiligheid, met het oog op het vergroten van de weerbaarheid van kennisinstellingen in het hoger onderwijs.

Het rapport maakt deel uit van een breder initiatief van het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) en kennisinstellingen om een robuust kader voor kennisveiligheid te ontwikkelen, te midden van de uitdagingen en kansen die de intensivering van internationale samenwerkingsverbanden met zich meebrengt. De internationale samenwerking in de kennissector is de afgelopen jaren sterk toegenomen, wat mede komt door de toegenomen mobiliteit. Wetenschappelijk onderzoek vereist vaak gespecialiseerde kennis en apparatuur die niet overal beschikbaar is. Door internationaal samen te werken, kunnen kennisinstellingen gebruikmaken van de middelen, kennis en vaardigheden van andere instellingen. Sommige onderzoeksprojecten worden daarnaast gefinancierd door internationale organisaties die grensoverschrijdende samenwerking vereisen. Instellingen kunnen door samen te werken gemakkelijker toegang krijgen tot deze fondsen. De vooruitgang in communicatie- en informatietechnologieën maakt internationale samenwerking bovendien gemakkelijker en goedkoper dan ooit tevoren. Deze groei brengt echter ook nieuwe risico's met zich mee, zoals ongewenste kennisoverdracht, heimelijke beïnvloeding en ethische kwesties, die de nationale veiligheid kunnen bedreigen. Deze risico’s zijn niet nieuw: zij bestaan reeds en gaan gepaard met de veranderende geopolitieke context. Door toenemende internationale samenwerking zijn deze risico’s echter ook in de kennissector steeds prominenter aanwezig.

1.1 Achtergrond

Begin 2022 is de Nationale Leidraad Kennisveiligheid gepubliceerd met als doel kennisinstellingen op weg te helpen om ervoor te zorgen dat internationale samenwerking veilig kan plaatsvinden (Ministerie van Onderwijs, Cultuur en Wetenschap, 2022). Deze leidraad is een gezamenlijk initiatief van Universiteiten van Nederland (UNL), de Koninklijke Nederlandse Akademie van Wetenschappen (KNAW), de Vereniging Hogescholen (VH), de Nederlandse Federatie van Universitair Medische Centra (NFU), de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO), de TO2-Federatie en de Rijksoverheid. De gids is gericht aan kennisinstellingen die te maken hebben met internationale samenwerking en daarbij kansen en risico’s tegen elkaar moeten afwegen. De leidraad is gecreëerd om bewustzijn rondom kennisveiligheid-vraagstukken te vergroten en geeft richting aan manieren waarop de weerbaarheid van kennisinstellingen vergroot kan worden. Deze leidraad maakt deel uit van een bredere inspanning van de Rijksoverheid om de kennisveiligheid in het land te versterken.

Analyses

De afgelopen twee jaar heeft een aantal initiatieven bijgedragen aan een groeiend beeld van de opgaven waar kennisinstellingen voor staan op het gebied van kennisveiligheid. In april 2022 heeft Minister Dijkgraaf van OCW een oproep gedaan aan Nederlandse kennisinstellingen om een risicoanalyse rond kennisveiligheid uit te voeren, met als doel de identificatie van gevoelige kennisgebieden en kroonjuwelen binnen de organisaties. Deze analyse is door de meeste universiteiten en hogescholen uitgevoerd.

Daarnaast heeft OCW onderzoeksbureaus Oberon en Dialogic gevraagd om onderzoek te doen naar het kennisveiligheidsbeleid van universiteiten en hogescholen. Dit heeft in oktober 2023 geresulteerd in het sectorbeeld universiteiten, waarin ook een aantal dilemma's ten aanzien van de verdere ontwikkeling van kennisveiligheid wordt benoemd. Op het moment van schrijven van dit rapport moet het sectorbeeld hogescholen en het sectorbeeld KNAW en NWO nog gepubliceerd worden.

De Adviesraad voor wetenschap, technologie en innovatie (AWTI) heeft bovendien in het voorjaar van 2022 een verkenning uitgevoerd naar de thematiek rondom kennisveiligheid. Deze verkenning omvat diverse analyses, waaronder een inventarisatie van risico's en dreigingen met betrekking tot kennisveiligheid. In het uiteindelijke AWTI advies 'Kennis in conflict – veiligheid en vrijheid in balans', gepubliceerd in december 2022, wordt onder anderen geadviseerd om een *capability maturity model* ofwel volwassenheidsmodel te implementeren. Dit is aanleiding voor OCW om een verkennend onderzoek te laten uitvoeren naar de toepasbaarheid van een capability maturity model op het gebied van kennisveiligheid bij kennisinstellingen.

1.2 Doelstelling van het onderzoek

Het voorliggende verkennend onderzoek heeft tot doel de toepasbaarheid van een volwassenheidsmodel op het gebied van kennisveiligheid bij kennisinstellingen te onderzoeken. Hierbij wordt onder anderen nader ingegaan op de definitie van een volwassenheidsmodel en hoe het van toegevoegde waarde zou kunnen zijn in de verdere ontwikkeling van kennisveiligheid.

Dit rapport geeft tevens de zienswijze weer van zowel Deloitte als kennisinstellingen ten aanzien van een dergelijk model, de voor- en nadelen van de toepassing van een volwassenheidsmodel in de context van kennisveiligheid. Tenslotte wordt er ingegaan op alternatieve manieren welke aansluiten bij de wens van OCW de kennisinstellingen zo goed mogelijk te ondersteunen bij het vergroten van de weerbaarheid op het gebied van kennisveiligheid.

Dit rapport fungeert als input voor OCW om te bepalen welke vervolgstappen genomen moeten worden in het verdere onderzoek naar het bevorderen van de weerbaarheid van kennisinstellingen op het gebied van kennisveiligheid. Het rapport beantwoordt de volgende vragen die door OCW zijn geformuleerd:

1. Wat is een volwassenheidsmodel?
2. Wat is de toepassing van een dergelijk model in de context van kennisveiligheid?
3. Hoe kan een volwassenheidsmodel bijdragen aan het verbeteren van de samenwerking tussen verschillende (integrale) veiligheidsdomeinen binnen instellingen?
4. Hoe kijken kennisinstellingen naar het ontwikkelen, implementeren en gebruiken van een dergelijk model? Wat zijn de voor- en nadelen van de toepassing van een volwassenheidsmodel ten behoeve van kennisveiligheid in het hoger onderwijs en onderzoek? En verschilt dat tussen instellingen?
5. Welke eisen stelt een optimale toepassing aan de inhoudelijke kenmerken en de implementatie van een model, zowel inhoudelijk als qua inbedding in bestaande instrumenten en processen in het bredere onderwijs- en onderzoekslandschap? Vereist dit een specifieke houding van OCW en kennisinstellingen? Verschilt dit per type instelling?

6. Hoe kan een volwassenheidsmodel bijdragen aan het verhogen van de weerbaarheid van kennisinstellingen? En hoe kan een volwassenheidsmodel de weerbaarheid van instellingen inzichtelijk maken voor verschillende typen risico's?
7. In hoeverre sluiten de toepassingsmogelijkheden van een model en de visie van de onderzoekers aan bij de wijze waarop de AWTI heeft geschetst dat het model toe te passen is?
8. Zijn er naast volwassenheidsmodellen eventueel andere modellen of methodieken die beter passen bij de behoefte en doelstellingen van OCW en de kennisinstellingen?

Vraag 1 wordt beantwoord in hoofdstuk 2. De vragen 2 t/m 8 worden beantwoord in hoofdstuk 3.

1.3 Aanpak van het onderzoek

De beantwoording van de door OCW geformuleerde vragen heeft plaatsgevonden volgens een methodologie die in overleg met OCW is toegepast. Een documentanalyse is verricht, waarvan een gedetailleerd overzicht is opgenomen in de bijlagen van dit rapport, aangevuld met voorbeelden uit de praktijk ten behoeve van de beantwoording van de onderzoeksvragen. Gesprekken zijn gevoerd met diverse belanghebbenden en vertegenwoordigers van koepels en kennisinstituten die door OCW zijn aangewezen. Een volledige lijst van deze gesprekspartners is eveneens in de bijlage gevoegd. De deelnemers, waaronder vertegenwoordigers van universiteiten, hogescholen, brancheverenigingen, SURF, OCW en de Koninklijke Nederlandse Akademie van Wetenschappen (KNAW), zijn geselecteerd op basis van hun betrokkenheid bij en kennis van integrale veiligheid en kennisveiligheid. De bevindingen verkregen uit deze dialogen zijn voor verificatie voorgelegd aan de deelnemers. Na deze bevestiging zijn de resultaten opgenomen in dit rapport.

Deloitte heeft de ontvangen informatie uit interviews en documentatie als juist en volledig aangenomen. Uitsluitend OCW is verantwoordelijk voor onder meer: (a) het nemen van alle managementbeslissingen, (b) het evalueren van de toereikendheid en de resultaten van het rapport, (c) het accepteren van de verantwoordelijkheid voor het gebruik van de resultaten van het rapport.

1.4 Scope van het onderzoek

Deze verkenning richt zich vooral op het onderzoeken van de toepasbaarheid van een volwassenheidsmodel op het gebied van kennisveiligheid bij kennisinstellingen. De term 'toepasbaarheid' in de context van deze opdracht verwijst naar de mate waarin een volwassenheidsmodel voor kennisveiligheid geschikt en effectief kan worden ingezet bij kennisinstellingen. Het gaat erom te bepalen of het volwassenheidsmodel kan worden gebruikt als een hulpmiddel of kader voor deze organisaties om hun kennisveiligheidsprocessen te beoordelen, te ontwikkelen en te verbeteren.

In deze verkenning wordt onder andere nader ingegaan op de definitie van een volwassenheidsmodel en hoe het van toegevoegde waarde kan zijn in de verdere ontwikkeling van kennisveiligheid. De term 'toegevoegde waarde' in deze context verwijst naar de extra voordelen of verbeteringen die een volwassenheidsmodel kan bieden in het streven naar verbeterde kennisveiligheid binnen een kennisinstelling. Het gaat over de manier waarop het aanwenden van een volwassenheidsmodel kan leiden tot meer dan alleen de basisfuncties van kennisveiligheid, en hoe het kan bijdragen aan verdere ontwikkeling en versterking van de kennisveiligheidspraktijken.

De verkenning heeft niet tot doel om niveaus binnen een model te specificeren of het inhoudelijk ontwikkelen van een volwassenheidsmodel. Ook wordt de potentiële rol van OCW in relatie tot de mogelijke verdere ontwikkeling van een volwassenheidsmodel niet gedefinieerd. Tot slot valt de implementatie van het volwassenheidsmodel bij onderwijsinstellingen buiten de scope van de voorverkenning.

1.5 Structuur van het rapport

In hoofdstuk *1. Introductie* wordt de achtergrond van het onderzoek beschreven en worden de vragen vanuit OCW uiteengezet. In hoofdstuk *2. Het volwassenheidsmodel* wordt de definitie beschreven van een volwassenheidsmodel, de toepassing in de praktijk en de voor- en nadelen van het gebruik van een volwassenheidsmodel. In hoofdstuk *3. De toepassing van een volwassenheidsmodel in de context van kennisveiligheid* wordt ingegaan op het vraagstuk hoe een volwassenheidsmodel de samenwerking tussen veiligheidsdomeinen eventueel kan verbeteren, hoe kennisinstellingen kijken naar de toepassing van een volwassenheidsmodel en de vraag in hoeverre hun visie hierop overeenkomt met de visie van de AWTI op een volwassenheidsmodel. In hoofdstuk *4. Conclusie* is een aantal belangrijke observaties opgenomen.

2. Het volwassenheidsmodel

In dit hoofdstuk wordt antwoord gegeven op onderzoeksvraag '*Wat is een volwassenheidsmodel?'.*

De aanpak wordt geïnitieerd met het presenteren van een definitie van het volwassenheidsmodel, gevolgd door een uiteenzetting van de bijbehorende doelstellingen. Aansluitend wordt de theorie geïllustreerd door middel van praktijkvoorbeelden. Concluderend vindt een evaluatie van de voordelen en beperkingen van het volwassenheidsmodel plaats, gebaseerd op een combinatie van literatuuronderzoek, de praktijk en inzichten verkregen uit interviews.

2.1 Wat is een volwassenheidsmodel?

Het volwassenheidsmodel of Capability Maturity Model komt van oorsprong uit de software-industrie in de jaren '80 en is ontwikkeld om de kwaliteit van software-ontwikkelprocessen te beoordelen, meten en vergelijken, gebruikmakend van een gemeenschappelijke taal en referentiepunt. Vanaf dat moment zijn volwassenheidsmodellen wereldwijd gebruikt in verschillende industrieën en is het een referentiekader geworden voor veel meer processen dan enkel software.

Een volwassenheidsmodel is een gestructureerd overzicht met meestal vijf niveaus, dat de voortgang van een organisatie bij het ontwikkelen van processen en vaardigheden weergeeft. Het heeft als doel vast te stellen in welke mate de huidige organisatiestructuur overeenkomt dan wel verschilt met de gewenste structuur. Door deze verschillen in kaart te brengen, kunnen organisaties gerichte verbeteringen doorvoeren, waarbij volwassenheid impliceert dat de organisatie geleidelijk naar de gewenste situatie evolueert.

De vijf niveaus van een volwassenheidsmodel, vaak toegepast in modellen zoals het Capability Maturity Model Integration (CMMI), beschrijven de gradaties van volwassenheid waardoor een organisatie kan meten en verbeteren hoe zij haar processen beheert. Elk niveau biedt een fundament voor de volgende stap in het streven naar verbeterde efficiëntie, effectiviteit en kwaliteit van de organisatieprocessen:

- *Niveau 1, initieel:* op dit niveau zijn processen veelal ad-hoc en weinig tot niet uitgewerkt. De organisatie heeft geen stabiele omgeving, waardoor prestaties onvoorspelbaar en reactief zijn.
- *Niveau 2, herhaalbaar:* de organisatie heeft enkele stabiele processen die projecten succesvol kunnen herhalen. Er is een basisniveau van projectmanagement dat zorgt voor enige consistentie in prestaties.
- *Niveau 3, gedefinieerd:* de organisatie heeft haar processen gedocumenteerd en gestandaardiseerd. Het management en de medewerkers begrijpen hun activiteiten en er is een organisatiebrede standaard voor processen.
- *Niveau 4, beheerst:* op dit niveau meet de organisatie haar processen en prestaties. Dit zorgt voor een proactieve benadering om processen te verbeteren met behulp van data en kwantitatieve technieken.
- *Niveau 5, optimaliserend:* de hoogste fase van volwassenheid waarbij de organisatie continu procesverbetering nastreeft.

Normenkader
Het volwassenheidsmodel kan zonder een specifiek normenkader functioneren als een zelfstandig hulpmiddel voor zelfevaluatie en verbetering. Echter, in de praktijk wordt het vaak gecombineerd met een normenkader om organisaties een duidelijk pad naar compliance en verbetering te bieden. Het model helpt organisaties begrijpen 'hoe' ze zich kunnen verbeteren, terwijl het normenkader aangeeft 'waaraan' ze moeten voldoen.

Het normenkader bestaat uit een reeks standaarden, richtlijnen en good practices (ook wel controls genoemd), gegroepeerd in domeinen (bijvoorbeeld governance, leveranciersmanagement e.d.) die zijn opgesteld om organisaties te helpen bij het bepalen van de gewenste normen voor hun processen en gedrag. Bij de toepassing van een volwassenheidsmodel fungeert het normenkader als een ankerpunt, waardoor organisaties hun status kunnen evalueren, doelgerichte verbeteringen kunnen aanbrengen en kunnen zorgen voor compliance met relevante standaarden en wetgeving.

Daarbij is het overigens mogelijk om, naar gelang de risico's in een organisatie, te kiezen voor verschillende volwassenheidsniveau's per domein. Een organisatie kan bijvoorbeeld de ambitie hebben om een gemiddeld volwassenheidsniveau van drie (van vijf) te behalen, waarbij een risicogebaseerde keuze wordt gemaakt voor een hoger dan wel lager volwassenheidsniveau voor bepaalde domeinen. Onder anderen beschikbare capaciteit, kennis en budget kunnen onderdeel zijn van deze risicoafweging en het gekozen tijdpad.

Risicobereidheid
Naarmate organisaties een hoger niveau van volwassenheid bereiken, worden ze vaak beter in staat om hun risicobereidheid te duiden en te beheren. Dit komt doordat volwassen organisaties doorgaans over meer ontwikkelde en verfijnde risicobeheersingsprocessen beschikken. Ze hebben duidelijke beleidslijnen, procedures en controlemechanismen die hen helpen bij het identificeren, beoordelen en mitigeren van risico's.

Op hogere volwassenheidsniveaus zijn organisaties meestal beter uitgerust om de impact en waarschijnlijkheid van risico's te analyseren, waardoor ze een meer genuanceerde kijk op risicobereidheid kunnen ontwikkelen. Ze zijn in staat om betere beslissingen te nemen over welke risico's acceptabel zijn in lijn met hun strategische doelstellingen en welke risico's vermeden of verkleind moeten worden. Bovendien zorgt een hoger niveau van volwassenheid voor een cultuur waarin risicomanagement een integraal onderdeel is van de dagelijkse bedrijfsvoering. In dergelijke organisaties is risicobewustzijn verspreid over alle lagen van de organisatie, van het management tot de werkvloer. Dit vergroot de kans dat risico's op tijd worden herkend en dat er adequaat op wordt gereageerd.

2.2 Toepassing in de praktijk
Volwassenheidsmodellen vinden hun toepassing in een breed scala van sectoren en disciplines, waar ze organisaties ondersteunen in het evalueren en verbeteren van hun bedrijfsprocessen.

2.2.1 Volwassenheidsmodellen voor verschillende disciplines
Om een paar voorbeelden te noemen: in de informatietechnologie worden modellen zoals het Capability Maturity Model Integration (CMMI) ingezet om de kwaliteit van softwareontwikkeling en IT-

servicebeheer te verhogen. Met de toenemende nadruk op cybersecurity maken organisaties gebruik van het Cybersecurity Maturity Model Certification (CMMC) om hun beveiligingsmaatregelen te beoordelen en te verbeteren. Bij het beheer van data biedt het Data Management Maturity (DMM) model een kader voor het optimaliseren van databeheer en -governance. En in bredere context zijn risicomanagementmodellen zoals het Risk Management Maturity Model (RMMM) ontworpen om organisaties te helpen bij het proactief identificeren en beheren van potentiële risico's.

De lijst gaat verder met volwassenheidsmodellen op het gebied van projectmanagement (OPM3), dienstverlening (Service Capability & Performance (SCP) Standards) en het Supply Chain Operations Reference (SCOR) model voor inkoop- en distributieprocessen. Ten slotte, in het streven naar duurzaamheid en milieuverantwoordelijkheid wordt het Sustainability Maturity Model (SMM) gebruikt om de prestaties op het gebied van milieubeheer te meten.

2.2.2 Volwassenheidsmodellen in het publieke domein

In het publieke domein faciliteren volwassenheidsmodellen eveneens de systematische verbetering van organisatorische processen, diensten en prestaties, door een duidelijk raamwerk te bieden voor evaluatie en ontwikkeling. Volwassenheidsmodellen zijn voor de overheid waardevolle hulpmiddelen voor het monitoren en controleren van de voortgang, waarbij regelmatige beoordelingen zorgen voor aanhoudende afstemming en aanpassingen waar nodig. Deze transparantie speelt een sleutelrol in de verantwoording die vanuit de overheid plaatsvindt, zowel aan bijvoorbeeld het parlement als het publiek, en draagt bij aan het bouwen van vertrouwen. Bovendien ondersteunen volwassenheidsmodellen een cultuur van continue verbetering, aangezien publieke organisaties worden aangemoedigd om steeds hogere niveaus van bekwaamheid te bereiken. Het integreren van deze modellen in beleidsvorming en strategische planning zorgt ervoor dat uitvoeringsplannen afgestemd zijn op de volwassenheidsdoelstellingen die veelal gezamenlijk zijn afgesproken.

NBA-LIO

Een voorbeeld van een volwassenheidsmodel in het publieke domein is het NBA-LIO volwassenheidsmodel. Bij de overheid dienen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen) te voldoen aan de Baseline Informatiebeveiliging Overheid (BIO). De Auditdienst Rijk (ADR) maakt sinds 2019 gebruik van het NBA-LIO volwassenheidsmodel voor het rijksbrede onderzoek naar de sturing en beheersing van informatiebeveiliging. De maatregelen worden gerelateerd aan verschillende normenkaders, waaronder de BIO, de ISO/IEC 27002:2013 standaard, maar ook IT-raamwerken als ITIL en COBIT.

Domein	Volwassenheidsniveau 1 **Initial** Beheersmaatregelen zijn niet of slechts gedeeltelijk gedefinieerd en/of worden op een inconsistente manier uitgevoerd en zijn sterk afhankelijk van individuen.	Volwassenheidsniveau 2 **Repeatable** Beheersmaatregelen bestaan en worden op een gestructureerde en consistente, maar informele manier uitgevoerd.	Volwassenheidsniveau 3 **Defined** Beheersmaatregelen zijn gedocumenteerd en worden op een gestructureerde en formele manier uitgevoerd. Uitvoering van de maatregelen is aantoonbaar, getest en effectief.	Volwassenheidsniveau 4 **Managed and measurable** De effectiviteit van beheersmaatregelen wordt periodiek beoordeeld en indien nodig verbeterd. Deze beoordeling is gedocumenteerd.	Volwassenheidsniveau 5 **Continuous improvement** Een bedrijfsbreed risico- en beheersprogramma voorziet in continue en effectieve beheersing en aanpak van risico's.
Governance	- Implementatie en uitvoering van activiteiten en maatregelen op het gebied van informatiebeveiliging en/of cybersecurity gebeurt ad hoc.	- Een strategie en visie is geformuleerd, maar is niet formeel vastgesteld.	- Strategie en visie zijn goedgekeurd door het senior management - Strategie en missie worden actief gecommuniceerd naar medewerkers, leveranciers en business partners.	- Strategie en visie is leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging en cybersecurity. - Indien van toepassing wordt vastgelegd hoe er in lijn met strategie en visie gewerkt wordt. - De geldigheid en uitvoerbaarheid van de strategie en visie wordt periodiek geverifieerd.	- De strategie geeft aan hoe IT de organisatie helpt haar doelstellingen te behalen. - Indien noodzakelijk worden strategie en visie bijgesteld om organisatiedoelstellingen en externe ontwikkelingen bij te houden.

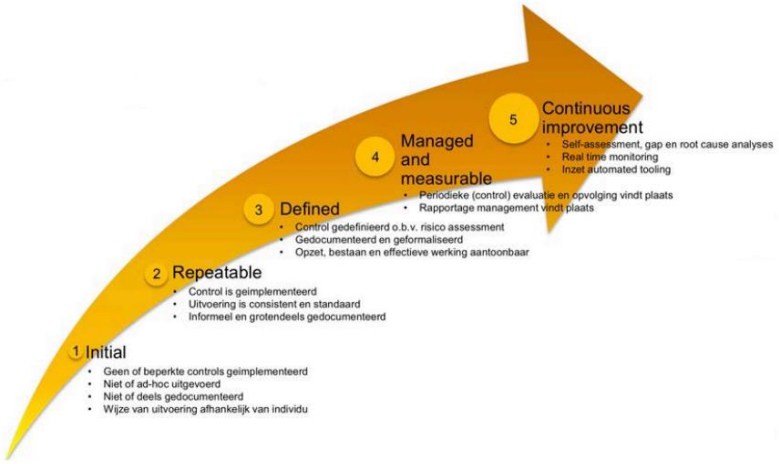
Figuur 1 *- Voorbeeld van het NBA-LIO volwassenheidsmodel (NOREA, 2019).*

De overheid stuurt inmiddels meer op feitelijke weerbaarheid door zich te richten op de vraag welk risico overblijft na implementatie van de BIO. Een self-assessment door de departementen, gericht op een selectie van de BIO, vormt de basis van een gesprek met de Auditdienst Rijk (ADR) over de mitigatie

van de onderkende risico's. Dit gesprek in de context van de planning- en controlcyclus is van groot belang, ook om helderheid te verkrijgen over de definitie en toepassing van de basisbeveiligingsniveaus binnen de BIO. Het gebruik van een spider diagram is hierbij een nuttig middel om de scores te verduidelijken en actie te ondernemen op basis van deze inzichten.

SURF

Een ander voorbeeld van een volwassenheidsmodel is het model van SURF (figuur 2), dat is gebaseerd op het NBA-LIO model. In combinatie met het SURFaudit Toetsingskader Informatiebeveiliging biedt dit model een leidraad en handvatten waarmee Nederlandse onderwijs- en onderzoeksinstellingen doelgericht en op pragmatische wijze hun organisaties kunnen ondersteunen bij het meten, bepalen en verbeteren van het volwassenheidsniveau van informatiebeveiliging. Naar aanleiding van onder anderen de ransomware-aanval op de Universiteit Maastricht in 2019 hebben alle Universiteiten en hogescholen afgesproken om toe te groeien naar volwassenheidsniveau drie van vijf.



Figuur 2 *- Voorbeeld van een volwassenheidsmodel, ontworpen door SURF (SURF, 2019).*

Naast een toetsingskader voor informatiebeveiliging heeft SURF een vergelijkbaar toetsingskader opgesteld voor privacy. Deze kaders stellen instellingen in staat de status van informatiebeveiliging en privacy te kwantificeren. Op basis van deze kwantificering kunnen instellingen maatregelen nemen die proportioneel zijn tot de geïdentificeerde risico's en daarmee de groei in volwassenheid op het gebied van informatiebeveiliging en privacy bewerkstelligen.

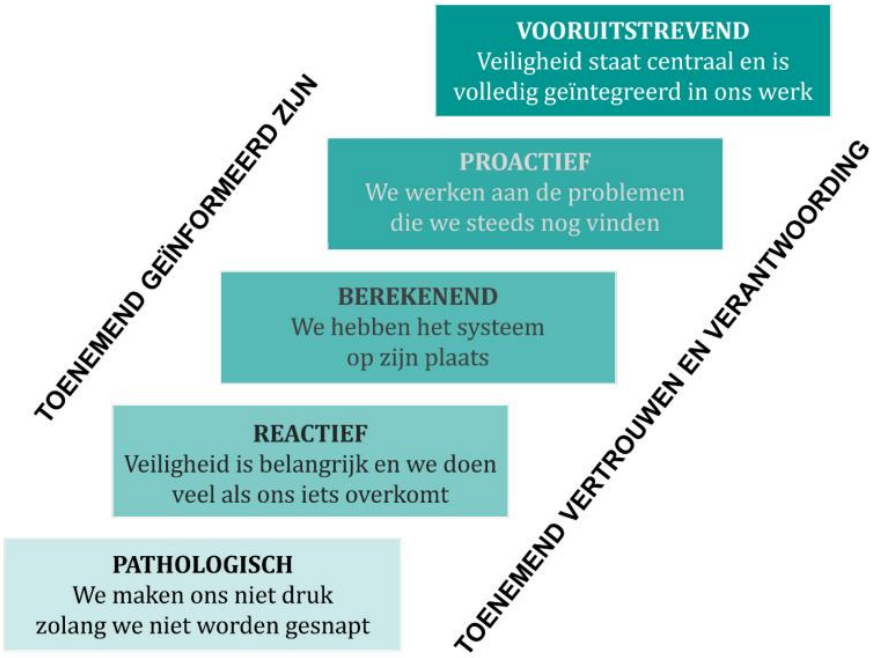
Safety Culture Ladder

De Safety Culture Ladder (SCL) is, net als de hiervoor genoemde instrumenten, een voorbeeld van een volwassenheidsmodel om een proces binnen organisaties te meten en te stimuleren. Het oorspronkelijk door ProRail ontwikkelde model is inmiddels in beheer genomen door NEN en wordt toegepast in allerlei verschillende sectoren waaronder onderwijs en gemeenten.

Ook de Safety Culture Ladder heeft als doel om organisaties te helpen om hun veiligheidscultuur te ontwikkelen en te verbeteren. Dit leidt tot een veiliger werkomgeving voor medewerkers, minder ongevallen en incidenten, en een hogere productiviteit. De SCL hanteert hiertoe vijf thema's, die verder zijn uitgewerkt in controls:

1 Beleid en leiderschap
2 Kennis en vaardigheden
3 Primaire en secundaire processen
4 Samenwerken met externen
5 Leren en verbeteren.

Het model maakt gebruik van vijf treden, die elk een niveau van veiligheidsbewustzijn vertegenwoordigen. Hoe hoger een organisatie op de ladder staat, hoe beter het is gesteld met de veiligheidscultuur. De definitie van de treden is vergelijkbaar met de modellen van overheid en SURF.



Figuur 3 – De Safety Culture Ladder 2.0: 2023 (NEN).

Organisaties kunnen zich laten certificeren op de SCL. Dit houdt in dat een onafhankelijke auditor de organisatie beoordeelt op basis van de vijf treden en de mate van volwassenheid per thema. De auditor bepaalt op welke trede de organisatie zich gemiddeld bevindt en geeft een certificaat uit.

2.3 De voor- en nadelen van een volwassenheidsmodel

Terwijl volwassenheidsmodellen worden geprezen voor hun vermogen om gestructureerde verbetering en standaardisatie van processen te bieden, is het van belang om een gebalanceerd beeld te vormen van wat dergelijke modellen in het algemeen in de praktijk betekenen. Aan de ene kant kunnen ze organisaties helpen hun (beveiligings)maatregelen te beoordelen en te optimaliseren, wat leidt tot verhoogde weerbaarheid en continuïteit. Aan de andere kant kunnen er uitdagingen en beperkingen zijn, zoals het ontbreken van de vereiste middelen voor implementatie en onderhoud, of de mogelijkheid dat een bijbehorend normenkader niet voldoende ruimte laat aan eigen invulling en daarmee niet goed aansluit bij de unieke behoeften van elke organisatie.

2.3.1 Voordelen

Objectieve beoordeling

De voordelen van het inzetten van volwassenheidsmodellen zitten in de mogelijkheid tot een objectieve beoordeling van de prestaties van processen en het aanreiken van methodische stappen voor het verbeteren van deze processen. Deze modellen zijn in tal van sectoren, waaronder de software- en informatiebeveiligingsindustrieën, erkend als krachtige instrumenten om de huidige staat van organisatorische processen te evalueren en verbetertrajecten voor te stellen richting een hogere mate van volwassenheid.

Verhoging van kwaliteit en productiviteit

De kwaliteit van processen neemt toe met name door het bieden van een raamwerk voor het vaststellen van prioriteiten en het volgen van ontwikkelingen. Hierdoor ontstaan er minder inconsistenties in de manier waarop binnen organisaties opvolging wordt gegeven aan onderkende risico's. Een normenkader verschilt daarin van bijvoorbeeld een kwaliteitskader in het achterliggende doel. Een normenkader is vaak gedetailleerd, voorschrijvend van aard en gericht op het naleven van bepaalde minimumeisen of regelgeving conform het 'pas toe of leg uit' principe. Een kwaliteitskader heeft veelal een bredere insteek en is meer gericht op het streven naar een hoger niveau van prestatie en klanttevredenheid, en niet zozeer strikte naleving.

Door de combinatie van een volwassenheidsmodel met een normenkader te vertalen naar een duidelijk gedefinieerde, gestructureerde aanpak die tegemoet komt aan de ambities en risico's in de eigen werkomgeving, ligt er bovendien een basis die helpt bij het verhogen van productiviteit: het biedt heldere richtlijnen ten aanzien van de aard en planning van maatregelen. Dit geeft ook richting aan de prioritering van maatregelen en de kosten die daarmee gemoeid zijn. Wanneer een organisatie duidelijke prioriteiten kan stellen, kunnen middelen (tijd, geld, personeel) effectiever worden toegewezen aan de belangrijkste taken en projecten. Dit vermijdt verspilling van middelen op minder kritieke of minder invloedrijke activiteiten. Inconsistenties in processen kunnen bovendien leiden tot fouten, vertragingen en herstelwerk. Door processen te standaardiseren en te verduidelijken, worden dergelijke inconsistenties verminderd, wat de efficiëntie verhoogt en de kwaliteit verbetert. Daarnaast ervaren medewerkers vaak meer betrokkenheid doordat duidelijk is wat de organisatie van ze verwacht.

Inzicht in de sector

Volwassenheidsmodellen spelen een cruciale rol in het faciliteren van benchmarking, waarbij organisaties de mogelijkheid krijgen om hun eigen prestaties en processen te spiegelen aan die van vergelijkbare organisaties binnen hun sector. Dit helpt organisaties om inzicht te verkrijgen in waar ze zich bevinden ten opzichte van de industrienormen, welke verbeteringen noodzakelijk zijn en hoe zij kunnen leren van de good practices die door anderen al succesvol zijn geïmplementeerd. Met deze kennis kunnen organisaties eventueel hun strategische doelen bijstellen en gerichte verbetertrajecten ontwerpen. Dit stimuleert niet alleen innovatie door organisaties aan te moedigen om creatieve oplossingen te vinden voor hun uitdagingen, maar het geeft ook inzicht in sectorbrede trends, zoals de adoptie van nieuwe technologieën of werkmethoden. Een voorbeeld is de inzet van interactieve media, virtual reality (VR) of kunstmatige intelligentie (AI) voor gepersonaliseerd leren.

Het gebruik van volwassenheidsmodellen als communicatiemiddel mag ook niet onderschat worden. Het stelt organisaties in staat om zowel intern als extern inzichtelijk te maken in hoeverre ze zich hebben ontwikkeld en hoe toegewijd ze zijn aan kwaliteit en continue verbetering. Dit kan bijdragen aan het versterken van het vertrouwen van investeerders, klanten en partners in de organisatie. Sterker nog, het kan bijdragen aan het versterken van vertrouwen in een volledige sector, indien organisaties gezamenlijk afspraken hebben gemaakt over het verhogen van hun ambitieniveau.

In de publieke sector stelt een volwassenheidsmodel de overheid in staat om vast te stellen hoe organisatie die onder hun toezicht vallen zich verhouden tot good practices en breed gehanteerde standaarden. Daarnaast is een volwassenheidsmodel een middel om te kunnen sturen, mits dit goed is ingebed in de manier waarop de overheid richting wil geven aan organisaties die binnen het betreffende werkveld vallen: het helpt bij het identificeren van risicovolle gebieden, waardoor de overheid toezichtsactiviteiten beter kan prioriteren en deze effectiever kunnen worden ingezet.

Het biedt tevens een basis voor verdere samenwerking: op basis van de inzichten uit het volwassenheidsmodel kan de overheid specifieke en bruikbare feedback verschaffen die organisaties helpt hun processen en compliance te verbeteren. Dit vergroot de transparantie omdat de criteria voor toezicht duidelijk worden gecommuniceerd en bevordert daarmee ook de duidelijkheid en eerlijkheid van het toezichtsproces.

2.3.2 Nadelen

Desalniettemin dragen volwassenheidsmodellen ook beperkingen met zich mee, zeker wanneer een dergelijk model niet wordt gezien als één van de middelen om verdere besluitvorming te faciliteren. Indien het management van een organisatie zich enkel richt op het nastreven van een hoger niveau van volwassenheid (‘afvinken’) zonder dit in de bredere context van de organisatie te plaatsen kan dit resulteren in een verwaarlozing van andere vitale elementen zoals organisatiecultuur, capaciteit tot leren en de kwaliteit van governance.

Organisatiecultuur

Volwassenheidsmodellen zijn ontworpen om de procesvolwassenheid binnen organisaties te evalueren en te verbeteren door te focussen op meetbare aspecten zoals gedocumenteerde procedures, naleving van standaarden en het behalen van prestatie-indicatoren. Organisatiecultuur is een meer impliciet, gedragsgebonden en minder tastbare aspect van een organisatie, wat het moeilijker meetbaar en kwantificeerbaar maakt. Het integreren van een zacht aspect zoals cultuur in een volwassenheidsmodel zou de complexiteit echter aanzienlijk verhogen. Het is uitdagend om een algemeen toepasbaar model te ontwikkelen dat rekening houdt met de unieke culturele aspecten van elke organisatie, terwijl dit sterk kan variëren afhankelijk van de organisatiegrootte, het type instelling, de historie en de sector.

Leervermogen

Volwassenheidsmodellen zijn vaak gestructureerd rond vaste processen en procedures, waardoor bestuurders en gebruikers zich kunnen blindstaren op compliance. Organisaties kunnen zich soms te veel richten op het voldoen aan de vereisten van een volwassenheidsmodel, waardoor het naleven van een checklist belangrijker wordt dan het daadwerkelijk verbeteren van de prestaties of het aanpakken van de onderliggende oorzaken van problemen. Het nastreven van verbeteringen om een hoger niveau in het volwassenheidsmodel te bereiken kan organisaties aanmoedigen om zich te richten op

kortetermijnwinsten in plaats van op langdurige ontwikkeling en leren. Wanneer de nadruk ligt op compliance boven begrip kan daarbij de situatie ontstaan waarin werknemers procedures volgen zonder de onderliggende principes en de reden voor bepaalde processen volledig te begrijpen. Deze rigiditeit kan innovatie en flexibiliteit beperken, wat nodig is voor effectief leren en aanpassen aan veranderende omstandigheden.

Kwaliteit van governance

Een dergelijke rigide aanpak kan tevens invloed hebben op de governance in een organisatie. Wanneer in de toepassing van een volwassenheidsmodel teveel de nadruk ligt op procesverbetering, kunnen belangrijke elementen van governance kwaliteit in de verdrukking komen. Bijvoorbeeld, effectief toezicht en strategische besluitvorming kunnen ondergeschikt raken aan het voldoen aan de eisen van het model. Dit kan ertoe leiden dat beslissingen worden genomen die weliswaar in lijn zijn met het model, maar die niet noodzakelijkerwijs het beste zijn voor de langetermijnstrategie van de organisatie. Daarnaast kan een organisatie met een sterke focus op compliance in eigen processen minder aandacht besteden aan het actief betrekken van externe samenwerkingspartners bij de besluitvorming, wat kan leiden tot een afname van vertrouwen en steun. Dit vraagt om een nadrukkelijke rol voor de leiders in een organisatie.

Hoewel inspirerend en effectief leiderschap onmiskenbaar een fundamentele rol speelt in goede governance, is het belangrijk om te erkennen dat dit soms kan worden ondergewaardeerd wanneer de focus te eenzijdig is gericht op procesverbetering. Procesverbeteringen zijn essentieel voor het verhogen van de efficiëntie en verminderen van kosten, maar een overmatige concentratie hierop kan inderdaad ten koste gaan van het investeren in leiderschapsontwikkeling.

Het is essentieel dat organisaties een evenwicht vinden tussen beide aspecten. Enerzijds moeten processen continu worden geëvalueerd en verfijnd om te verzekeren dat de organisatie zo doeltreffend mogelijk werkt. Anderzijds moeten leiderschapscapaciteiten worden ontwikkeld en onderhouden, aangezien leiders de cultuur vormen, medewerkers motiveren, en de organisatie door veranderingen leiden met een duidelijke visie en missie.

3. De toepassing van een volwassenheidsmodel in de context van kennisveiligheid

In dit hoofdstuk wordt de onderzoeksvraag *'Wat is de toepassing van een dergelijk model in de context van kennisveiligheid?'* behandeld.

3.1 Integrale veiligheid

Deze paragraaf geeft antwoord op de vraag:

Hoe kan een volwassenheidsmodel bijdragen aan het verbeteren van de samenwerking tussen verschillende (integrale) veiligheidsdomeinen binnen instellingen?

De gesprekken met diverse kennisinstellingen hebben een belangrijk inzicht aan het licht gebracht: kennisveiligheid wordt algemeen beschouwd als een essentiële component van het beleid ten aanzien van integrale veiligheid (IV). Het belang dat aan dit aspect wordt gehecht, reflecteert de groeiende erkenning van het feit dat intellectueel eigendom, onderzoeksdata en de algehele veiligheid van kennis binnen de institutionele grenzen, cruciaal zijn voor het voortbestaan en de vooruitgang van kennisinstellingen.

Thema's als crisisbeheer, informatiebeveiliging en privacy nemen een centrale plek in binnen de veiligheidsagenda en worden vaak in één adem genoemd met kennisveiligheid. Dit komt doordat deze domeinen niet in isolatie functioneren; de bescherming van gevoelige informatie is in veel gevallen verbonden met privacykwesties, en effectief crisisbeheer is vaak afhankelijk van robuuste veiligheidsprotocollen. De interactie tussen deze domeinen leidt tot een integrale aanpak waarbij de versterking van één aspect tot verbeteringen leidt in de andere. Instellingen erkennen daarbij dat het waarborgen van kennisveiligheid verder gaat dan enkel technische maatregelen; het behelst een strategische benadering die samenwerking vereist tussen verschillende afdelingen, zoals IT, human resources, juridische zaken en onderzoekers.

Een facet dat in de gesprekken nadrukkelijk naar voren kwam, is de mate van samenwerking tussen deze domeinen. De samenwerkingsverbanden binnen instellingen zijn volgens de gesprekspartners al sterk en blijven groeien, zowel op operationeel als op strategisch niveau. In dit kader wordt ook de cruciale rol van training en bewustwording benadrukt. Medewerkers moeten worden opgeleid om de principes van kennisveiligheid te begrijpen en correct toe te passen binnen hun dagelijkse werkzaamheden. Daarnaast bestaan er in bredere zin verschillen tussen instellingen in de mate waarin risicomanagement is ingericht. Niet iedereen is bijvoorbeeld even ervaren in het inzichtelijk maken van risico's of het is niet volledig duidelijk waar de besluitvorming ligt ten aanzien van risico's. Een cultuur van veiligheidsbewustzijn draagt bij aan het verminderen van risico's en het versterken van de organisatorische veerkracht.

Kennisinstellingen zijn verdeeld over de vraag of een volwassenheidsmodel de samenwerking tussen deze domeinen nog verder kan verbeteren. Gespreksdeelnemers vanuit zowel universiteiten als hogescholen staan terughoudend tegenover een dergelijk model, met name omdat het gezien wordt als manier om vanuit de overheid toezicht uit te voeren bij instellingen. Echter vanuit met name de groep managers integrale veiligheid (vanuit zowel hogescholen als universiteiten) wordt een

volwassenheidsmodel gezien als een manier om in bredere zin dan enkel kennisveiligheid het onderwerp veiligheid naar een hoger niveau te tillen. Daarbij zou de focus vooral moeten liggen op het steviger neerzetten van risicomanagement. Het vermogen om risico's in te schatten varieert volgens de IV'ers aanzienlijk binnen instellingen, waardoor de roep om duidelijkheid te scheppen over verantwoordelijkheden in het risicobeheersingsproces sterker is geworden. Er is een behoefte aan een integrale methodiek die niet alleen helpt bij het inschatten van risico's, maar ook bij het begrijpen van de verantwoordelijkheden binnen het risicobeheerproces. Onderdeel hiervan is bijvoorbeeld de manier om risico's en kansen evenwichtig te beoordelen, met de nadruk op de verantwoordelijkheid van de eerste lijn: de wetenschappers zelf.

3.2 De toepassing van een volwassenheidsmodel voor kennisveiligheid

Deze paragraaf geeft antwoord op de vragen:

Hoe kijken kennisinstellingen naar het ontwikkelen, implementeren en gebruiken van een dergelijk model? Wat zijn de voor- en nadelen van de toepassing van een volwassenheidsmodel ten behoeve van kennisveiligheid in het hoger onderwijs en onderzoek? En verschilt dat tussen instellingen?

De respons vanuit het werkveld op het gebruik van volwassenheidsmodellen voor kennisveiligheid is behoorlijk eensgezind. Aan de positieve zijde erkennen professionals het nut van een volwassenheidsmodel voor het verfijnen van de aanpak per onderzoeksgroep, wat bijdraagt aan een beter afgestemde en methodische benadering van kennisveiligheid binnen de organisatie. Een volwassenheidsmodel kan helpen bij het bepalen van prioriteiten binnen het veiligheidsbeleid en bij het volgen van progressie door het stellen van duidelijke en meetbare doelen. Deze modulaire aanpak maakt het mogelijk om gerichte verbeteringen aan te brengen en verschaft een instrument om successen te identificeren en te vieren. Indien er gekozen wordt voor de toepassing van een volwassenheidsmodel, achten kennisinstellingen het echter van belang dat er een duidelijk normenkader is, net als bij de Algemene Verordening Gegevensbescherming (AVG) voor privacy en ISO 27001/2 voor informatiebeveiliging, en dat er geen dubbel werk met andere kaders ontstaat. Door betrokkenheid van de gebruikers bij de ontwikkeling te vergroten, neemt bovendien het draagvlak toe.

Echter, de delicate balans tussen het handhaven van academische vrijheid en de bescherming van de wetenschap tegen ongewenste kennisoverdracht, heimelijke beïnvloeding en ethische kwesties stelt een uitdaging voor kennisinstellingen die zowel openheid als bescherming van gevoelige informatie nastreven. Het beeld lijkt te bestaand dat een volwassenheidsmodel met normenkader vooral een auditinstrument is dat gericht is op compliance en daarbij te weinig ruimte biedt aan een diverse benadering van risico's en bijbehorende mitigerende maatregelen. Daarmee zou een volwassenheidsmodel geen recht doen aan de diversiteit van risicoprofielen en behoeften van verschillende instellingen of – zelfs nog een stap verder – afzonderlijke faculteiten en onderzoeksgroepen. De waardevolle aspecten van internationale samenwerking en uitwisseling van kennis zouden bovendien onderbelicht kunnen raken. Dit is met name benadrukt door universiteiten.

De beleving van kennisinstellingen is dat volwassenheidsmodellen teveel focussen op het monitoren en meten van processen, wat ten koste kan gaan van daadwerkelijke innovatie en verbetering. De

nadruk kan verschuiven naar het voldoen aan de criteria van het model, in plaats van naar het echt vooruit helpen van de organisatie op het gebied van kennisveiligheid. Dit kan resulteren in een bureaucratische oefening in plaats van een middel tot wezenlijke verbetering van veiligheidscultuur en -praktijken. Een strikt model beperkt daarmee de flexibiliteit in het implementeren van maatregelen.

Bovendien maken kennisinstellingen zich zorgen over de complexiteit die kan ontstaan wanneer verantwoordelijkheden over meerdere rollen en domeinen worden verdeeld. Dit kan leiden tot verwarring over wie waarvoor verantwoordelijk is en tot een verhoogde administratieve last.

Kennisinstellingen geven ook aan dat ze actief betrokken willen zijn bij het verbeteren van kennisveiligheid, waarbij de nadruk ligt op de ontwikkeling van tools ten behoeve van de daadwerkelijk uitvoering van taken in plaats van het meten van vooruitgang. Bij zowel universiteiten als hogescholen lijkt het beeld te bestaan dat de overheid veel vraagt van kennisinstellingen, maar onvoldoende houvast biedt voor besluitvorming over risico's in onderwijs en onderzoek. Een voorbeeld is de mogelijke weigering van bepaalde gastdocenten of promovendi op basis van geconstateerde risico's, terwijl niet duidelijk is welke juridische basis hieraan ten grondslag ligt. Daarnaast hebben instellingen behoefte aan duidelijkheid over rollen en verantwoordelijkheden in het duiden van en besluiten over risico's door overheid en instellingen. Zowel universiteiten als hogescholen en koepels zien daarin een leidende rol door de overheid, specifiek OCW in het faciliteren en richting geven, maar ook door te ondersteunen in de ontwikkeling van tools en instellingen te stimuleren om daarmee actief aan de slag te gaan.

Over de ontwikkeling van een volwassenheidsmodel zijn kennisinstellingen het eens dat een uniform model voor alle instellingen geen doel op zich is. Desondanks en om kennisveiligheid te verbeteren is een werkgroep vanuit de universiteiten gestart en inmiddels vergevorderd in de ontwikkeling van een eigen volwassenheidsmodel.[1] Hogescholen zijn hier tot op heden echter niet bij betrokken. De meerderheid lijkt van mening te zijn dat een volwassenheidsmodel op dit moment enkel gebruikt zou kunnen worden als een leermiddel en gespreksstarter en niet als een strikte maatstaf. Wat betreft de toegevoegde waarde van inzicht in de sector geven instellingen aan dat dit besproken wordt in de werkgroep kennisveiligheid. Hier zijn hogescholen echter niet vertegenwoordigd.

3.3 Eisen aan een volwassenheidsmodel

Deze paragraaf geeft antwoord op de vragen:

Welke eisen stelt een optimale toepassing aan de inhoudelijke kenmerken en de implementatie van een model, zowel inhoudelijk als qua inbedding in bestaande instrumenten en processen in het bredere onderwijs- en onderzoekslandschap? Vereist dit een specifieke houding van OCW en kennisinstellingen? Verschilt dit per type instelling?

Bij de eventuele inzet van een volwassenheidsmodel binnen het onderwijs- en onderzoekslandschap is het essentieel dat zowel de inhoudelijke eigenschappen van het model als de wijze van implementatie nauwkeurig worden afgestemd op de unieke behoeften van het hoger onderwijs en wetenschap. Een doeltreffend volwassenheidsmodel dient niet alleen als een meetinstrument, maar ook als een

1 Ten tijde van het gesprek met de koepels en universiteiten was dit model nog niet gereed en daarmee de inhoud niet bekend bij Deloitte.

katalysator voor continue verbetering en ontwikkeling. Hieropvolgend verkennen we de specifieke eisen die gesteld worden aan een optimaal volwassenheidsmodel en hoe deze succesvol kan worden verankerd in de bestaande instrumenten en processen van onderwijs- en onderzoeksinstellingen. We richten ons hierbij op de inhoudelijke kenmerken die een model effectief en relevant maken, en op de implementatieaspecten die cruciaal zijn om het model naadloos te laten aansluiten bij en ondersteunend te maken aan de bestaande praktijken en ambities van deze instellingen op het gebied van kennisveiligheid.

3.3.1 Inhoudelijke kenmerken

Het volwassenheidsmodel moet relevant en *toepasbaar* zijn op de specifieke context van de onderwijs- en onderzoekssector. Hierin is de mening van hogescholen en universiteiten gelijk. Dit houdt in dat het model de unieke aspecten van academische culturen, onderwijspraktijken en onderzoeksactiviteiten moet kunnen adresseren. Daarnaast moet het model voldoende *flexibel* zijn om aan te sluiten bij de diversiteit van instellingen binnen het onderwijs en onderzoekslandschap en moet ruimte bieden voor maatwerk in implementatie en evaluatie. Om ook tegemoet te kunnen komen aan de behoefte van OCW om inzicht te krijgen in verschillen en overeenkomsten binnen de onderwijssector moeten criteria en indicatoren in het model meetbaar en observeerbaar zijn, zodat vooruitgang objectief kan worden vastgesteld en gemonitord. Een holistische benadering van volwassenheid is van belang, die zo *volledig* mogelijk is en alle belangrijke aspecten van organisatieprestaties omvat, inclusief onderwijskwaliteit, onderzoeksexcellentie, kennisuitwisseling, managementprocessen en governance. Dit is met name benoemd door de managers integrale veiligheid, gezien het belang om risicomanagement goed in te richten.

Tenslotte moet het model gericht zijn op *continue verbetering*, niet alleen op compliance, en organisaties stimuleren om proactief processen te verbeteren en te innoveren. Dit is met name een belang van kennisinstellingen, maar volgens Deloitte ook inherent onderdeel van de methodiek om volwassenheid te vergroten. Onderdeel van een volwassen aanpak om risico's te onderkennen en mitigeren is het stimuleren van het lerende vermogen van een organisatie, wat onder anderen kan leiden tot het inzicht dat innovatie bepaalde processen soepeler kan laten verlopen.

3.3.2 Inbedding in bestaande instrumenten en processen

Om effectief te zijn moet een volwassenheidsmodel geïntegreerd worden met bestaande strategieën, plannen, en kwaliteitszorginstrumenten die al in gebruik zijn binnen onderwijs- en onderzoeksinstellingen. Met name universiteiten benoemen dit punt in de context van het verlagen van de auditlast. De implementatie van het model vereist daarbij een ondersteunende organisatiecultuur die waarde hecht aan kwaliteitsverbetering, leren en ontwikkeling. Bestuurders, docenten en onderzoekers dienen betrokken te worden in het proces om draagvlak maar ook eigenaarschap te genereren. Met name wetenschappers en docenten hebben op de werkvloer te maken met kennisveiligheid, zij het niet altijd op dagelijkse basis. Onderzoekers en ondersteunende medewerkers hebben voldoende kennis en vaardigheden nodig om met een volwassenheidsmodel te kunnen werken. Dit kan betekenen dat er investeringen nodig zijn in professionalisering en scholing. Dit vraagt inspanning van zowel OCW (o.a. overbrengen van de rol van kennisveiligheid in de context van nationale veiligheid) als kennisinstellingen (o.a. inbedden van kennisveiligheid in bestaande (risicomanagement) processen).

3.3.3 Rollen en verantwoordelijkheden van overheid en instellingen

Een volwassenheidsmodel dient in overeenstemming te zijn met zowel nationale als internationale wetgeving, accreditatievereisten en de specifieke richtlijnen die gelden voor onderwijs- en onderzoeksinstellingen. Het is daarbij essentieel dat de verantwoordelijkheden van OCW helder zijn, evenals wat er van de kennisinstellingen zelf wordt verwacht. Zowel universiteiten als hogescholen hebben de noodzaak aangegeven voor duidelijke kaders die door OCW worden gesteld ten aanzien van de reikwijdte van deze verantwoordelijkheden, onderwerpen waar kennisveiligheid met name van belang is en de manier waarop risico's gewogen dienen te worden. Een expliciete afbakening van deze verantwoordelijkheden is van cruciaal belang. Het stelt het bestuur van de instellingen in staat om zichtbaar en actief deel te nemen aan de invoering van het model, de noodzaak ervan te benadrukken en de benodigde middelen vrij te maken. Dit is van belang vanwege onder anderen het gegeven dat het nemen van maatregelen op het gebied van (kennis)veiligheid door sommige wetenschappers wordt ervaren als een inbreuk op academische vrijheid en het doorbreken van het principe van Open Science. Dit proces vereist ook een effectieve communicatiestrategie over de doelstellingen, de voordelen en de functionaliteit van het volwassenheidsmodel. Op die manier wordt gewaarborgd dat alle betrokken partijen inzien hoe hun bijdrage het realiseren van de doelstellingen van het model, namelijk het verhogen van de weerbaarheid op het gebied van kennisveiligheid, ondersteunt.

3.4 Verhogen van de weerbaarheid

Deze paragraaf geeft antwoord op de vragen:

Hoe kan een volwassenheidsmodel bijdragen aan het verhogen van de weerbaarheid van kennisinstellingen? En hoe kan een volwassenheidsmodel de weerbaarheid van instellingen inzichtelijk maken voor verschillende typen risico's?

3.4.1 Verhogen van de weerbaarheid

Een volwassenheidsmodel kan aanzienlijk bijdragen aan het verhogen van de weerbaarheid van kennisinstellingen door hen te voorzien van een gestructureerd kader voor het analyseren, beoordelen en verbeteren van hun interne processen en beleid op het gebied van kennisveiligheid. Deze modellen stellen instellingen in staat om hun huidige prestatieniveaus te identificeren, kritieke zwakke punten te erkennen en gerichte verbeteringen door te voeren. Door het vaststellen van duidelijke en meetbare doelstellingen, kunnen instellingen hun vooruitgang systematisch volgen en zich aanpassen aan veranderingen in hun omgeving. Daarnaast bevordert het gebruik van een volwassenheidsmodel binnen een organisatie het bewustzijn en begrip van best practices en normen die van toepassing zijn binnen de sector. Deze moeten er overigens dan wel zijn. Dit bewustzijn is essentieel om proactief risico's te managen en de capaciteit om te reageren op onverwachte gebeurtenissen te verbeteren. Door een cultuur van continue verbetering te stimuleren, moedigt een volwassenheidsmodel medewerkers aan om voortdurend te zoeken naar manieren om de efficiëntie en effectiviteit van hun werkzaamheden te verhogen.

Een volwassenheidsmodel kan ook de samenwerking en communicatie tussen verschillende afdelingen versterken, wat leidt tot een meer geïntegreerde en samenhangende aanpak van uitdagingen op het gebied van kennisveiligheid. Dit is cruciaal om de veerkracht van de instelling te waarborgen; afdelingen en teams die goed op elkaar zijn afgestemd, kunnen efficiënter en effectiever reageren op crises. Daarbij zou het normenkader wel moeten voorzien in een onderdeel dat toeziet op de inrichting van

een duidelijke governance-structuur, die zorgt voor een heldere verantwoordelijkheidsverdeling en een verantwoordingscultuur binnen de organisatie bevordert. Dit zorgt ervoor dat beslissingen snel en op een geïnformeerde basis gemaakt kunnen worden, wat van essentieel belang is in tijden van crisis.

In het algemeen draagt de toepassing van een volwassenheidsmodel bij aan de opbouw van een robuuste instelling die niet alleen in staat is om huidige uitdagingen aan te gaan, maar ook om toekomstige bedreigingen te anticiperen en zich daarop voor te bereiden. Dit verhoogt de algehele weerbaarheid en stelt de instelling in staat om haar strategische doelen te blijven nastreven, zelfs onder moeilijke omstandigheden.

Kennisinstellingen zijn echter van mening dat een separaat volwassenheidsmodel voor kennisveiligheid niet per se nodig is om deze weerbaarheid te bewerkstelligen. Ze hechten meer waarde aan praktische tools en bewustwording. Vanuit het oogpunt van integrale veiligheid is daarnaast gewezen op het belang om in algemene zin risicomanagement goed in te richten zodat, ongeacht het type risico, binnen onderwijsinstellingen een heldere structuur bestaat waarbij de inventarisatie, beoordeling en besluitvorming over risico's op het juiste niveau plaatsvindt. De ervaring van Deloitte is dat een volwassenheidsmodel weldegelijk kan bijdragen aan de weerbaarheid van instellingen, mits het bijgaand normenkader en fasering ten behoeve van invoering van een dergelijke systematiek goed is afgestemd op de behoeften van de diverse kennisinstellingen. Een volwassenheidsmodel geeft ruimte aan organisaties om zelf richting te geven

3.4.2 Inzichtelijk maken van de weerbaarheid per type risico

Een volwassenheidsmodel met betrekking tot kennisveiligheid kan specifiek afgestemd worden om risico's zoals ongewenste kennisoverdracht, heimelijke beïnvloeding en ethische kwesties aan te pakken. Een bijgaand normenkader kan deze thema's expliciet adresseren. Hieronder wordt uitgewerkt hoe een volwassenheidsmodel deze specifieke risico's kan adresseren:

Ongewenste kennisoverdracht - De dreiging van ongewenste kennisoverdracht houdt in dat gevoelige informatie illegaal wordt verworven door onbevoegde partijen, vaak voor concurrentievoordeel of andere strategische doeleinden. Een volwassenheidsmodel kan helpen bij het identificeren van kwetsbaarheden in de fysieke en digitale beveiliging van een kennisinstelling, het beoordelen van de effectiviteit van bestaande tegenmaatregelen en het verstrekken van een pad voor versterking van de bescherming van intellectueel eigendom door middel van onder anderen geavanceerde bewaking, netwerkbeveiliging en toegangscontroles.

Heimelijke beïnvloeding - Dit risico omvat pogingen van externe entiteiten om ongemerkt beleid, opinies of besluitvorming binnen een organisatie te sturen. Een resultaat kan zelfcensuur zijn. Een volwassenheidsmodel kan kennisinstellingen ondersteunen bij het ontwikkelen van een gedegen beleid voor transparantie, het invoeren van strikte protocollen voor belangenconflicten en het opzetten van trainingen die medewerkers leren om mogelijke beïnvloedingspogingen te herkennen en hierop te reageren.

Ethische kwesties – Samenwerking met collega's in landen waar grondrechten niet gerespecteerd worden, kan risico's opleveren wanneer onderzoekers betrokken raken bij de ontwikkeling van methodes of technologieën die worden ingezet voor bijvoorbeeld de onderdrukking van burgers. Een

volwassenheidsmodel kan kennisinstellingen helpen om hun huidige praktijken (voortdurend) kritisch te evalueren, met name hoe ze omgaan met internationale samenwerkingsverbanden, de vraag of ze nog steeds voldoen aan zowel de ethische normen van de instelling als de bredere maatschappelijke verwachtingen en de selectie van partners.

Bij elk van deze specifieke risico's kan een volwassenheidsmodel een rol spelen bij het vaststellen van een algehele cultuur van veiligheid en waakzaamheid binnen de organisatie. Het gaat niet alleen om de implementatie van technische maatregelen, maar ook om het ontwikkelen van (risicomanagement)beleid en procedures die zorgen voor een robuuste governancestructuur en een sterk bewustzijn bij onderzoekers en andere betrokkenen.

3.5 Volwassenheidsmodel in relatie tot het AWTI-advies

Deze paragraaf geeft antwoord op de vraag:

In hoeverre sluiten de toepassingsmogelijkheden van een model en de visie van de onderzoekers aan bij de wijze waarop de AWTI heeft geschetst dat het model toe te passen is?

Het advies van de AWTI duikt diep in het proces van het implementeren van een volwassenheidsmodel voor kennisveiligheid. Het benadrukt hoe zo'n model kan worden toegesneden op de specifieke veiligheidsbehoeften van verschillende domeinen binnen een organisatie. Dit vereist een gedetailleerde analyse van elk domein om te bepalen welke risico's aanwezig zijn en welke maatregelen nodig zijn om deze risico's te mitigeren. Het gaat hierbij niet alleen om het in kaart brengen van risico's, maar ook om het ontwikkelen van een systeem waarin maatregelen aangepast worden aan de mate waarin een risico zich voordoet. Dit impliceert een grondige kennis van de operationele context van elk functioneel onderdeel van de organisatie, waaronder het type onderzoek, de mogelijke toepassingen van de geproduceerde kennis, en de aard van de samenwerkingsverbanden. De AWTI lijkt daarmee alle lagen van de organisatie als doelgroep te zien. Het is echter de vraag of het realistisch is om van iedere medewerker te verwachten dat hij/zij in staat is om in de implementatie te werken met een volwassenheidsmodel. In de praktijk blijkt bijvoorbeeld veelal weinig ruimte voor onderzoekers te zijn voor werkzaamheden anders dan het bedrijven van wetenschap en komt het hanteren van een volwassenheidsmodel vooral neer bij een select aantal medewerkers dat hierin gespecialiseerd is.

Essentieel in deze aanpak is de samenwerking met externe partijen, zoals veiligheidsdiensten en ministeries, die cruciale kennis en expertise kunnen inbrengen. De input van deze stakeholders is van vitaal belang om het model zowel effectief als legitiem te maken. Dit duidt op een proces waarbij openbare en niet-openbare informatie wordt verzameld en geïntegreerd om een uitgebreid en accuraat beeld te vormen van de kennisveiligheidslandschap. Het model bevordert ook een gelaagde aanpak, die het mogelijk maakt om te escaleren en samen te werken met externe partijen indien de situatie dat vereist.

Het advies van de AWTI sluit grotendeels aan bij de visie op de toepassingsmogelijkheden van volwassenheidsmodellen van Deloitte, echter deze verkenning onderstreept het belang van het creëren van een cultuur waarin bewustzijn van good practices en normen wordt aangemoedigd. Door deze benadering worden medewerkers gestimuleerd om continu naar efficiëntie en effectiviteit te streven.

Dit draagt bij aan de organisatorische veerkracht, omdat het niet alleen gaat om het aanpakken van huidige risico's en uitdagingen, maar ook om het proactief voorbereiden op toekomstige dreigingen.

Bovendien benadrukt deze verkenning het belang van samenwerking en communicatie tussen afdelingen binnen een instelling om een geïntegreerde aanpak van kennisveiligheid te waarborgen. Het stelt dat een volwassenheidsmodel kan helpen bij het opzetten van een duidelijke governance-structuur die een heldere verantwoordelijkheidsverdeling en een sterke verantwoordingscultuur bevordert. Dit is cruciaal voor het maken van snelle en goed geïnformeerde beslissingen, vooral in tijden van crisis.

Waar de AWTI zich richt op de specifieke en praktische implementatie van maatregelen in response op geïdentificeerde risico's, richt deze verkenning zich meer op het ontwikkelen van een adaptieve en leergerichte organisatie die voortdurend streeft naar verbetering. Hier wordt een volwassenheidsmodel gezien als een middel om het bewustzijn te verhogen en een cultuur te creëren die niet alleen gericht is op compliance, maar ook op het overstijgen van basisnormen en het streven naar een optimale aanpak in kennisveiligheid.

3.6 Alternatieven

Deze paragraaf geeft antwoord op de vraag:

Zijn er naast volwassenheidsmodellen *eventueel andere modellen of methodieken die beter passen bij de behoefte en doelstellingen van OCW en de kennisinstellingen?*

In deze verkenning naar de toepassing van een volwassenheidsmodel om kennisveiligheid binnen kennisinstellingen te verhogen, is benoemd dat een dergelijk model doorgaans gepaard gaat met een normenkader: een bredere set van richtlijnen, principes, standaarden en best practices die gebruikt worden om de kwaliteit en integriteit van processen of activiteiten te waarborgen. Het gaat om een overkoepelende structuur die de visie, waarden en algemene doelstellingen van een organisatie of sector weergeeft. Een normenkader biedt ruimte voor interpretatie, zodat organisaties het kunnen aanpassen aan hun specifieke context. Het dient als referentiepunt voor het maken van beslissingen en het ontwikkelen van procedures en beleid. Normenkaders worden vaak gebruikt om compliance te beoordelen, waarbij de nadruk ligt op het volgen van geaccepteerde normen en het bereiken van bepaalde uitkomsten, zonder strikt te zijn in hoe die uitkomsten behaald moeten worden. Daarmee is een volwassenheidsmodel in combinatie met een eigen normenkader het uitgangspunt voor deze verkenning.

Er zijn echter alternatieve scenario’s om kennisveiligheid naar een hoger niveau te tillen, welke allemaal de nodige voor- en nadelen kennen.

Scenario 1 Eisen met betrekking tot kennisveiligheid

Als (minder flexibel) alternatief voor een normenkader kan een specifieke en gedetailleerde opsomming van vereisten en voorwaarden worden opgesteld waaraan voldaan moet worden. Hierbij zou deels gebruik gemaakt kunnen worden van normeringen als ISO, met de kanttekening dat dit mogelijk tot overlap leidt met al in gebruik zijnde normenkaders, waar nodig aan te vullen met nieuw op te stellen eisen. Een eis is doorgaans concreet en meetbaar, en laat minder ruimte voor

interpretatie. Een dergelijke lijst met eisen kan bijvoorbeeld betrekking hebben op technische specificaties, juridische voorwaarden, of beleidsmatige verplichtingen die helder en expliciet beschreven zijn om de exacte verwachtingen en deliverables vast te stellen. Door middel van een audit wordt de compliance getoetst, waarbij het niet voldoen aan de eisen de nodige nadelige gevolgen voor de organisatie heeft. Hoewel dit ruimte biedt aan OCW om grip te krijgen op de mate waarin kennisveiligheid door kennisinstellingen is ingericht, is voor hen een set harde eisen met audit niet gewenst vanwege het gebrek aan ruimte voor eigen interpretatie.

Scenario 2 Bundeling van audits

Een benadering die tegemoet komt aan de wens van kennisinstellingen om niet een apart volwassenheidsmodel met normenkader en bijbehorende audit te introduceren, is de Eenduidige Normatiek Single Information Audit (ENSIA). Deze norm biedt ruimte voor autonomie en beperkt daarnaast de auditlast door een aantal IT-audits te bundelen. ENSIA onderscheidt zich van een standaard audit door zijn specifieke toepassing in de Nederlandse publieke sector, met name bij gemeenten. Het combineert verschillende IT-audits en vragenlijsten in een gestroomlijnde aanpak die gemeenten helpt om aan verschillende informatieveiligheidsnormen te voldoen. In tegenstelling tot de traditionele audits waar externe auditors de leiding hebben, beginnen gemeenten binnen ENSIA met een zelfevaluatie en stellen vervolgens een bestuurlijk verantwoordingsrapport op.

ENSIA legt de focus op horizontale verantwoording, wat inhoudt dat de gemeenteraad actief betrokken is bij het proces, dit in tegenstelling tot de verticale verantwoording van een standaard audit die vaak gericht is op het hogere management of toezichthouders. Daarnaast stimuleert ENSIA een dialoog binnen gemeenten om de informatieveiligheid continu te verbeteren, een aspect dat verder gaat dan de feitelijke constateringen van een standaard audit. ENSIA biedt gemeenten ook de flexibiliteit om zich te concentreren op de voor hen meest relevante risico's en verbeterpunten, terwijl standaard audits over het algemeen een vaststaand raamwerk hanteren.

Voor audits in de domeinen informatiebeveiliging, privacy en kennisveiligheid kan ENSIA fungeren als leidraad om de verschillende relevante normenkaders, zoals de SURF toetsingskaders voor cybersecurity en privacy en eventuele kennisveiligheidsnormen, samen te voegen tot één coherente set van vereisten. Door de principes van ENSIA toe te passen, kunnen audits voor informatiebeveiliging, privacy en kennisveiligheid meer gestroomlijnd en geïntegreerd worden uitgevoerd, wat leidt tot een duidelijker overzicht van de stand van zaken en een gerichtere aanpak van verbeteringen op deze gebieden. Dit draagt niet alleen bij aan de naleving van regelgeving, maar bevordert ook een cultuur van continue verbetering en bewustzijn rondom belangrijke veiligheidsaspecten binnen kennisinstellingen.

Scenario 3 Volwassenheidsmodel met normenkader als leermiddel

Een suggestie die regelmatig de revue is gepasseerd in de gesprekken, is om in eerste instantie te focussen op het verder toerusten van kennisinstellingen om kennisveiligheid sterk neer te zetten in de eigen organisatie, alvorens aan de slag te gaan met een groei in volwassenheid en benchmarking. Een normenkader zou als leermiddel hierin kunnen ondersteunen. In deze aanpak kan bijvoorbeeld gekozen worden voor enkel zelfassessments en het delen van onderlinge uitkomsten, waarbij in een later stadium gekozen kan worden voor compliancegericht toezicht.

Een volwassenheidsmodel kan dienen als een krachtig leermiddel dat organisaties begeleidt in een proces van zelfevaluatie, waarbij instellingen hun huidige praktijken en resultaten spiegelen aan de beschrijvingen binnen het model. Dit bevordert een grotere bewustwording van het belang van bepaalde processen en de omgang met risico's (zowel binnen kennisinstellingen als in de interactie met externe partners) en draagt bij aan het creëren van een gedetailleerd ontwikkelingsplan. Door dit plan krijgen instellingen een heldere route voor het stapsgewijs verbeteren van processen op het gebied van kennisveiligheid (en zelfs breder) en het invoeren van nieuwe praktijken. Dit vraagt wel de nodige inspanning en kennis van instellingen om risico's goed te kunnen inventariseren en waarderen.

Bovendien functioneert het model als een feedbackloop, die niet alleen de voortgang van verbeteringen meet, maar ook waardevolle inzichten terugkoppelt naar de organisatie. Dit voedt een continu leerproces, waarbij acties en doelstellingen regelmatig worden geëvalueerd en bijgesteld. Het delen van kennis, zowel binnen de organisatie als met externe partijen, wordt ook gefaciliteerd door het model, wat leidt tot een cultuur van collectieve verbetering en samenwerking.

Door te benadrukken dat het gebruik van een volwassenheidsmodel dialoog en interactie tussen verschillende teams en domeinen in de context van integrale veiligheid kan stimuleren, verbetert het samenspel op het gebied van risicomanagement binnen de organisatie en wordt iedereen aangemoedigd om mee te denken over verbetermogelijkheden. De ambitie om hogere niveaus van volwassenheid te bereiken kan organisaties inspireren om buiten de gebaande paden te denken en te streven naar innovatieve oplossingen die de interne processen verder kunnen verbeteren.

4. Conclusie

Op basis van de uitvoerige verkenning heeft dit rapport de toegevoegde waarde van de toepassing van een volwassenheidsmodel op het gebied van kennisveiligheid kritisch onderzocht, met een bijzondere focus op het versterken van de weerbaarheid van kennisinstellingen in het hoger onderwijs en wetenschap.

De bevindingen wijzen op een potentiële bijdrage van een dergelijk model aan de verbetering van kennisveiligheidspraktijken. Door een structuur te bieden voor het systematisch beoordelen en verhogen van procesvolwassenheid, kan het model helpen om risico's zoals ongewenste kennisoverdracht, heimelijke beïnvloeding en ethische kwesties te adresseren. Dit is vooral relevant gezien de huidige trend van intensievere internationale samenwerking binnen de kennissector. Het volwassenheidsmodel kan als instrument dienen om strategische prioriteiten te stellen, te benchmarken met peers en helderheid te creëren in de verdeling van verantwoordelijkheden tussen OCW en de instellingen zelf (bijvoorbeeld door verwijzingen naar richtlijnen op te nemen in het normenkader). Het bevordert ook de zichtbare betrokkenheid van leiderschap bij de verdere ontwikkeling van kennisveiligheid en draagt bij aan een grotere betrokkenheid van medewerkers door duidelijke verwachtingen te stellen.

Desalniettemin worden ook de beperkingen en uitdagingen van een volwassenheidsmodel erkend. De diversiteit in risicoprofielen tussen verschillende kennisinstellingen en zelfs tussen faculteiten binnen dezelfde instelling stelt specifieke eisen aan de aanpasbaarheid en toepasbaarheid van een uniform model. Daarnaast is er een risico dat de nadruk op procesverbetering kan leiden tot een verwaarlozing van elementen zoals organisatorische cultuur, leervermogen en governancekwaliteit.

In het licht van deze bevindingen ligt de mogelijke toegevoegde waarde van een volwassenheidsmodel in de capaciteit van kennisinstellingen om een gebalanceerde benadering van kennisveiligheid te hanteren. Een benadering die niet alleen technische en procesgerichte aspecten omvat, maar ook rekening houdt met culturele, strategische en gedragsgerelateerde factoren. Het model zou kunnen functioneren als een dynamisch leermiddel dat bijdraagt aan een cultuur van continue verbetering, waarbij de focus ligt op ontwikkeling en innovatie in plaats van compliance en vinkjes zetten. Het zou daarnaast zoveel mogelijk moeten aansluiten bij bestaande volwassenheidsmodellen en normenkaders, zoals door SURF ontwikkeld op het gebied van informatiebeveiliging en privacy.

Het rapport benadrukt de noodzaak van een op maat gemaakte uitvoering, die rekening houdt met de unieke behoeften van elke instelling, de koepels, de overheid en andere belanghebbenden. Dit vraagt om flexibiliteit in zowel de inhoud als de uitvoering van het model en de nadrukkelijke betrokkenheid van alle stakeholders, inclusief OCW, bij het ontwikkelingsproces. Met deze aanpak kan een volwassenheidsmodel een kader bieden voor kennisinstellingen om hun weerbaarheid te versterken en de uitdagingen en kansen van internationale wetenschappelijke samenwerking in een steeds complexere wereld aan te gaan. De implementatie van een volwassenheidsmodel, ook als het als leermiddel dient, zal echter de nodige inspanningen vragen bij instellingen. Het gaat niet alleen om het leveren van praktische ondersteuning in de uitvoering, maar ook om het creëren van draagvlak onder onderzoekers en andere medewerkers en het (h)erkennen van risico’s voor de continuïteit en integriteit

van onderwijs en onderzoek alsmede de nationale veiligheidsagenda. Door het leiden van deze inspanningen en het waarborgen van de samenwerking met Europese partners, kan de overheid de academische wereld ondersteunen in het veiligstellen van hun kennis en technologieën. Hierdoor wordt een fundament gelegd voor toekomstige groei en succes, terwijl de nationale belangen beschermd blijven.

Bronnen

Bosma, B. (2019). *SURFaudit benchmark 2019 – rappor*. SURF. Geraadpleegd op 6 maart 2024, van https://www.surf.nl/files/2020-04/surfaudit-benchmark-2019-rapport-v1-def.pdf

Framework Knowledge Security Dutch Universities door de VSNU

Kennis in conflict - veiligheid en vrijheid in balans door het AWTI in november 2022

Kennisveiligheid - position paper door de KNAW in oktober 2023

Kennisveiligheid in hoger onderwijs en wetenschap door het Rathenau Instituut in januari 2021

Kennisveiligheidsbeleid in het hoger onderwijs en onderzoek door Oberon en Dialogic in september 2023

Microsoft. (2024, 10 januari). *CmMI (Capability Maturity Model Integration), achtergrondnotities - Azure Boards*. Microsoft Learn. Geraadpleegd op 20 februari 2024, van https://learn.microsoft.com/nl-nl/azure/devops/boards/work-items/guidance/cmmi/guidance-background-to-cmmi?view=azure-devops

Ministerie van Onderwijs, Cultuur en Wetenschap. (2022, 14 januari). *Nationale leidraad kennisveiligheid - Veilig internationaal samenwerken*. Rapport | Rijksoverheid.nl. Geraadpleegd op 21 februari 2024, van https://www.rijksoverheid.nl/documenten/rapporten/2022/01/14/nationale-leidraad-kennisveiligheid

Nationale Leidraad Kennisveiligheid door de Rijksoverheid in januari 2022

NBA-LIO. (2019, januari). *Handreiking bij Volwassenheidsmodel Informatiebeveiliging*. Nederlandse Beroepsorganisatie van Accountants. Geraadpleegd op 6 maart 2024, van https://www.nba.nl/siteassets/over-de-nba/ledengroepen/lio/lio-new/nba-lio-norea-handreiking-bij-volwassenheidsmodel-informatiebeveiliging-januari-2019.pdf

Safety Culture Ladder. (2023, september). *Safety Culture Ladder 2.0*. Geraadpleegd op 6 maart 2024, van https://safetycultureladder.com/app/uploads/2023/11/Normtekst-SCL__DEF_NL.pdf

Safety Culture Ladder. (z.d.). *Safety Culture Ladder (Veiligheidsladder) van NEN*. Geraadpleegd op 6 maart 2024, van https://safetycultureladder.com/

Sectorbeeld kennisveiligheid universiteiten door het Ministerie van OCW in oktober 2023

SURF. (z.d.). *SURF Coöperatie*. SURF.nl. Geraadpleegd op 20 februari 2024, van https://www.surf.nl/over-surf

Tarhan, A., Turetken, O., & Reijers, H. A. (2016). Business process maturity models: A systematic literature review. Information and Software Technology, 75, 122-134.

Tweede Kamer der Staten-Generaal. (2020, 18 december). *Informatie over Kamerstuk 31288, nr. 893 | Overheid.nl > Officiële bekendmakingen*. Overheid.nl. Geraadpleegd op 21 februari 2024, van https://zoek.officielebekendmakingen.nl/dossier/kst-31288-893

Bijlage A: Gesprekspartners

Adviesraad voor wetenschap, technologie en innovatie
Dialogic
Haagse Hogeschool
Hogeschool Nijmegen/Arnhem
Hogeschool Rotterdam
Ministerie van Onderwijs, Cultuur en Wetenschap
Nederlandse Federatie van Universitair Medische Centra
NHL Stenden Hogeschool
Koninklijke Nederlandse Akademie van Wetenschappen
SURF
Technische Universiteit Delft
Universiteit van Amsterdam
Universitair Medisch Centrum Groningen
Universiteit Twente
Universiteit Leiden
Universiteit Utrecht
Universiteiten van Nederland
Vereniging Hogescholen

Bijlage B: Afkortingenlijst

ADR	Auditdienst Rijk
ASPI	Australian Strategic Policy Institute
AWTI	Adviesraad voor wetenschap, technologie en innovatie
AVG	Algemene Verordening Gegevensbescherming
BIO	Baseline Informatiebeveiliging Overheid
CMMI	Capability Maturity Model Integration
CMMC	Cybersecurity Maturity Model Certification
DMM	Data Management Maturity
ENSIA	Eenduidige Normatiek Single Information Audit
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
KNAW	Koninklijke Nederlandse Akademie van Wetenschappen
LIO	Landelijk Informatiebeveiligingsbeleid Overheid
NBA	Nederlandse Beroepsorganisatie van Accountants
NFU	Nederlandse Federatie van Universitair Medische Centra
NWO	Nederlandse Organisatie voor Wetenschappelijk Onderzoek
OCW	Ministerie van Onderwijs, Cultuur en Wetenschap
OPM3	Organizational Project Management Maturity Model
RMMM	Risk Management Maturity Model
SCL	Safety Culture Ladder
SCP	Service Capability & Performance
SCOR	Supply Chain Operations Reference model
SMM	Sustainability Maturity Model
SURF	Samenwerkende Universitaire Rekenfaciliteiten
TO2-Federatie	Toegepast-Onderzoekorganisaties Federatie
UNL	Universiteiten van Nederland (voorheen VSNU)
VSNU	Vereniging van Samenwerkende Nederlandse Universiteiten

De verkenning wordt niet uitgevoerd in het kader van een assurance-opdracht zoals gedefinieerd in het International Framework for Assurance Engagements van de International Federation of Accountants (“IFAC”). Het is de verantwoordelijkheid van de (geautoriseerde) gebruikers van dit rapport om te beoordelen of deze in het perspectief van het geheel van de hen ter beschikking staande informatie en hun risicoperceptie aan de door hen te stellen eisen voldoen.

Dit rapport is bedoeld voor intern gebruik door OCW ten behoeve van het doel zoals omschreven in de opdrachtbevestiging met referentienummer IUCN23090014, gedateerd 10 december 2023. OCW zal Deloitte informeren indien dit rapport, dan wel delen daarvan, gedeeld wordt met derden dan wel gepubliceerd wordt.