Ministerie van Onderwijs, Cultuur en Wetenschap

Ontvangen: 3-5-2023 2023/018--

>Retouradres Postbus 16375 2500 BJ Den Haag

Saxion Hogeschool
T.a.v. het College van Bestuur
Postbus 70000
7500 KB ENSCHEDE

**Hoger Onderwijs en Studiefinanciering**
Rijnstraat 50
Den Haag
Postbus 16375
2500 BJ Den Haag
www.rijksoverheid.nl

**Onze referentie**
38115964

**Bijlagen**
1

*Als u belang hebt bij dit besluit, dan kunt u hiertegen binnen 6 weken, gerekend vanaf de verzenddatum, bezwaar maken. Stuur uw bezwaarschrift naar DUO, Postbus 30205, 2500 GE Den Haag. U kunt uw bezwaar ook digitaal indienen op www.bezwaarschriftenocw.nl.*

Datum 3 mei 2023
Betreft Besluit macrodoelmatigheid hbo associate degree-opleiding Cybersecurity

Geacht bestuur,

Met de brief van 7 maart 2023, door de Commissie Doelmatigheid Hoger Onderwijs (hierna: CDHO) ontvangen op 9 maart 2023, hebt u mij het voornemen voorgelegd om de hbo associate degree-opleiding Cybersecurity als bekostigde opleiding te verzorgen in Apeldoorn.

**Advies CDHO**
De CDHO heeft mij bij brief van 17 april 2023, kenmerk 2023/018, negatief geadviseerd over uw aanvraag. Dit advies, dat integraal deel uitmaakt van dit besluit, treft u hierbij aan.

**Besluit**
Gelet op het bovengenoemd advies van de CDHO, het bepaalde in de Wet op het hoger onderwijs en wetenschappelijk onderzoek (hierna: WHW) en in de Regeling macrodoelmatigheid hoger onderwijs (hierna: Regeling), heb ik besloten niet in te stemmen met uw voornemen om de hbo associate degree-opleiding Cybersecurity als bekostigde opleiding te verzorgen in Apeldoorn.

**Beoordelingskader**
De wettelijke grondslag voor mijn besluitvorming is gelegen in artikel 6.2 van de WHW. Voorts is de Regeling leidraad geweest voor mijn afwegingen.

**Motivering**
Overeenkomstig het advies van de CDHO concludeer ik dat uw aanvraag voldoet aan criterium a van artikel 4, eerste lid, van de Regeling, maar niet aan criterium b, eerste lid van dat artikel van de Regeling. Voor de nadere motivering verwijs ik u naar het advies van de CDHO.

Een afschrift van deze brief is verzonden aan de CDHO, de NVAO, DUO-Groningen, de Inspectie van het Onderwijs en de VH.

**Onze referentie**
38115964

Met vriendelijke groet,

de minister van Onderwijs, Cultuur en Wetenschap,
namens deze,
de directeur Hoger Onderwijs en Studiefinanciering,

Commissie
Doelmatigheid
Hoger Onderwijs

Ministerie van Onderwijs, Cultuur en Wetenschap
T.a.v. de Minister
Dhr. dr. R.H. Dijkgraaf
Postbus 16375
2500 BJ DEN HAAG

*Postadres*
Postbus 85498
2508 CD Den Haag
*Bezoekadres*
Parkstraat 83
2514 JG Den Haag
T: 070 8505300
W: www.cdho.nl
E: info@cdho.nl

| *Onderwerp* | *Ons Kenmerk* | *Datum* |
|---|---|---|
| Nieuwe opleiding<br>Saxion Hogeschool<br>Voltijd hbo Associate degree<br>Cybersecurity<br>Apeldoorn | 2023/018 | 17/04/2023 |

Geachte heer Dijkgraaf,

Op 09/03/2023 heeft de Commissie Doelmatigheid Hoger Onderwijs het voornemen ontvangen van Saxion Hogeschool om de hbo Associate degree Cybersecurity als bekostigde opleiding te verzorgen te Apeldoorn (brief van 07/03/2023 zonder kenmerk). De aanvraag was voorzien van alle voor de beoordeling benodigde gegevens en is door de commissie in behandeling genomen.

**Advies Commissie Doelmatigheid Hoger Onderwijs**
Gelet op het hiernavolgende adviseert de commissie u om negatief te besluiten op het verzoek van Saxion Hogeschool om de hbo Associate degree Cybersecurity als bekostigde opleiding te Apeldoorn te verzorgen.

**Beoordelingskader**
De wettelijke grondslag voor dit advies is gelegen in art. 6.2 van de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW). Voorts heeft de Regeling macrodoelmatigheid hoger onderwijs van 20 juni 2018, verder te noemen de Regeling, voor de commissie als leidraad gediend. Het beoordelingskader treft u in de bijlage bij dit advies aan.

**Omschrijving van de aanvraag**
De aanvrager wil de opleiding Cybersecurity in Apeldoorn aanbieden. Het gaat om een Nederlandstalige hbo Associate degree (hierna ook: Ad) die de aanvrager in het Croho onderdeel Techniek wil laten registreren. De voorgenomen opleiding omvat 120 studiepunten en de aanvrager wil deze in voltijdvorm aanbieden. De Ad Cybersecurity is opgebouwd uit drie leerlijnen: Basiskennis, Verdieping en Beroepspraktijk.

De leerlijn Basiskennis bestaat uit de drie hoofdthema's Operating Systems (Microsoft & Linux), Network Infrastructure & Security en Coding/Scripting (Python). De leerlijn Verdieping bestaat uit zes onderwerpen: Ethical Hacking, Web Applications, Security Monitoring, Security Governance, Threat Intelligence en een keuzevak. In de leerlijn Beroepspraktijk werken studenten aan opdrachten die ze in de beroepspraktijk kunnen tegenkomen. Afgestudeerde Cybersecurity specialisten zijn verantwoordelijk voor het beschermen van een organisatie tegen cyberdreigingen en datalekken. De opleiding is toegankelijk voor studenten met een mbo4-, havo- of vwo-diploma. Afgestudeerden van de beoogde opleiding kunnen aan het werk als (pen)tester, SOC analist/operator, adviseur, ethical hacker, security architect, security consultant, security engineer, information security officer, cloud engineer, cloud consultant, datacenter medewerker en netwerkbeheerder in verschillende sectoren, waaronder de financiële dienstverlening, gezondheidszorg, retail en overheid.

**Motivering**
De aanvraag voldoet naar mening van de commissie aan criterium a, maar niet aan criterium b in art. 4 lid 1 van de Regeling. De kern van de afwijzing berust op de constatering dat de bestaande opleidingen reeds kunnen voorzien in de arbeidsmarktbehoefte die de aanvrager aannemelijk heeft gemaakt. Er is derhalve geen ruimte om deze opleiding aan het bestaande aanbod toe te voegen.

*Beoordeling criterium a*
De aanvrager stelt dat de hbo Associate degree Cybersecurity aansluit op een arbeidsmarktbehoefte in combinatie met een maatschappelijke behoefte.

Beoordeling arbeidsmarktbehoefte
Ter onderbouwing van de arbeidsmarktbehoefte beroept de aanvrager zich op de prognoses voor opleidingstypen en beroepsgroepen zoals deze zijn opgenomen in het AIS van het ROA, de 'Monitor creatieve industrie 2021' van Media Perspectives (2021), het artikel 'Cyber security sector zoekt in krappe arbeidsmarkt hoogopgeleid personeel' van VPN Gids (2 maart 2023), de barometer 'ICT beroepen: Barometer Arbeidsmarkt' van het UWV (2021), het artikel 'De meest kansrijke banen van 2022' van Randstad (20 januari 2022), het overzicht van 'Kansrijke beroepen' van het UWV (2022), de 'IT arbeidsmarktmonitor 2021' van Hello Professionals (2022), het vacatureplatform Indeed.nl (februari 2023), het Dashboard Vacaturemarkt van het UWV (www.werk.nl/arbeidsmarktinformatie/dashboards/vacaturemarkt) en het arbeidsmarktonderzoek 'Doelmatigheidsonderzoek voor een voltijd Associate degree opleiding Cybersecurity' dat door Tien Organisatieadvies is uitgevoerd in opdracht van de aanvrager (2023).

De aanvrager beschouwt het opleidingstype bachelor informatica dat is opgenomen in het AIS van het ROA als relevant voor de voorgenomen opleiding Cybersecurity. De commissie deelt deze mening en acht dit opleidingstype het meest relevant omdat onder meer de aanverwante hbo Ad-opleidingen ICT, ICT-Beheer, IT Service Management en Informatica hierin zijn opgenomen. ROA typeert de vooruitzichten in 2026 voor afgestudeerden van dit opleidingstype als goed en verwacht grote knelpunten in de toekomstige personeelsvoorziening (zie Tabel 1).

Tabel 1. Arbeidsmarktprognoses opleidingstype bachelor informatica

| Opleidingstype | Arbeidsmarktprognose variabele | Indicator | Aantal | Totaal % 6 jr. | Gem. jaarlijks % | Typering |
|---|---|---|---|---|---|---|
| > > Bachelor - informatica | verwachte uitbreidingsvraag tot 2026 | | 9400 | 10 | 1.6 | erg hoog |
| > > Bachelor - informatica | verwachte vervangingsvraag tot 2026 | | 15500 | 17 | 2.6 | gemiddeld |
| > > Bachelor - informatica | verwachte baanopeningen tot 2026 | | 25000 | 27 | 4 | gemiddeld |
| > > Bachelor - informatica | verwachte instroom van schoolverlaters tot 2026 | | 15600 | 17 | 2.6 | gemiddeld |
| > > Bachelor - informatica | ITKP toekomstige knelpunten personeelsvoorziening in 2026 | 0.92 | | | | groot |
| > > Bachelor - informatica | ITA toekomstige arbeidsmarktsituatie in 2026 | 0.93 | | | | goed |

*Bron: ROA, AIS*

De aanvrager beroept zich tevens op de prognoses van het ROA voor de beroepsgroep databank- en netwerkspecialisten. De commissie kent in beginsel meer gewicht toe aan de prognoses voor opleidingstypen omdat daarin de uitstroom uit een cluster verwante opleidingen wordt gerelateerd aan verwachte baanopeningen voor dit type afgestudeerden.
De commissie acht met de aanvrager de beroepsgroep databank- en netwerkspecialisten relevant omdat afgestudeerden van de voorgenomen opleiding in aanmerking komen voor een deel van de beroepen binnen deze beroepsgroep, zoals systeembeheerders en netwerkspecialisten. Uit de prognoses van het ROA blijkt dat er voor deze beroepsgroep grote knelpunten in de toekomstige personeelsvoorziening worden verwacht (zie Tabel 2).

Tabel 2. Arbeidsmarktprognoses beroepsgroep databank- en netwerkspecialisten

| Beroepsgroep | Arbeidsmarktprognose variabele | Indicator | Aantal | Totaal % 6 jr. | Gem. jaarlijks % | Typering |
|---|---|---|---|---|---|---|
| Databank- en netwerkspecialisten | verwachte uitbreidingsvraag tot 2026 | | 8200 | 11 | 1.8 | erg hoog |
| Databank- en netwerkspecialisten | verwachte vervangingsvraag tot 2026 | | 8100 | 11 | 1.8 | laag |
| Databank- en netwerkspecialisten | verwachte baanopeningen tot 2026 | | 16300 | 23 | 3.5 | gemiddeld |
| Databank- en netwerkspecialisten | ITKB toekomstige knelpunten beroepsgroep in 2026 | 0.832 | | | | groot |

*Bron: ROA, AIS*

De commissie acht met de aanvrager de beroepsgroep software- en applicatieontwikkelaars eveneens relevant omdat afgestudeerden van de voorgenomen opleiding in aanmerking komen voor meerdere van de beroepen binnen deze beroepsgroep, zoals softwareontwikkelaars en systeemanalisten en ICT-adviseurs. Uit de prognoses van het ROA blijkt dat er voor deze beroepsgroep grote knelpunten in de toekomstige personeelsvoorziening worden verwacht (zie Tabel 3).

Tabel 3. Arbeidsmarktprognoses beroepsgroep software- en applicatieontwikkelaars

| Beroepsgroep | Arbeidsmarktprognose variabele | Indicator | Aantal | Totaal % 6 jr. | Gem. jaarlijks % | Typering |
|---|---|---|---|---|---|---|
| Software- en applicatieontwikkelaars | verwachte uitbreidingsvraag tot 2026 | | 31400 | 12 | 1.9 | erg hoog |
| Software- en applicatieontwikkelaars | verwachte vervangingsvraag tot 2026 | | 15900 | 6 | 1 | erg laag |
| Software- en applicatieontwikkelaars | verwachte baanopeningen tot 2026 | | 47300 | 18 | 2.7 | laag |
| Software- en applicatieontwikkelaars | ITKB toekomstige knelpunten beroepsgroep in 2026 | 0.802 | | | | groot |

*Bron: ROA, AIS*

De aanvrager heeft verder de prognoses voor de bedrijfssector informatie en communicatie in de arbeidsmarktregio Stedendriehoek en Noordwest Veluwe uit het AIS van het ROA in het dossier opgenomen. De commissie is van mening dat er te veel niet en nauwelijks relevante subsectoren in dit cluster zijn opgenomen en er wordt geen onderscheid gemaakt op opleidingsniveau. De commissie laat de prognoses voor deze bedrijfssector daarom buiten beschouwing.
De aanvrager doet verder een beroep op de prognoses voor de opleidingssubsector bachelor techniek en ict in de arbeidsmarktregio Stedendriehoek en Noordwest Veluwe. De commissie is van mening dat de opleidingssubsectoren zoals deze zijn opgenomen in het AIS te veel niet en nauwelijks relevante opleidingen bevatten en daardoor geen representatief beeld geven van de specifieke arbeidsmarkt waar afgestudeerden van de voorgenomen opleiding werkzaam zullen zijn. Om deze reden laat de commissie de prognoses voor deze opleidingssubsector buiten beschouwing.

De commissie concludeert dat de prognoses die zijn opgenomen in het AIS van het ROA voor het opleidingstype en de beroepsgroepen die relevant zijn voor de onderhavige opleiding een positief beeld geven van de arbeidsmarktperspectieven voor afgestudeerden van de voorgenomen opleiding Cybersecurity.

De aanvrager verwijst ook naar de 'Monitor creatieve industrie 2021' van Media Perspectives (2021, p. 6, 18, 21, 23 en 25) waarin een overzicht wordt gegeven van de arbeidsmarktontwikkelingen in de ICT-sector over de periode 2010-2020. Het rapport vermeldt onder meer dat het aantal ICT-bedrijven in deze periode is gestegen van ongeveer 28.000 naar ongeveer 81.900 en dat het ICT-aandeel op het totaal van Nederlandse bedrijven 4,6% is. Ook is in deze periode het aantal banen in de sector jaarlijks met gemiddeld 1,7% gestegen, wat hoger is dan het landelijk gemiddelde van 0,8%. Deze groei komt voornamelijk uit de bedrijfstakken facilitaire ICT-diensten en software. Specifiek voor de bedrijfstak software is de jaarlijkse groei van het aantal banen over deze periode 2,6% geweest. De commissie constateert dat deze bron voor wat betreft de onderzochte periode blijk geeft van een groeiende arbeidsmarkt in de sector waar afgestudeerden van de voorgenomen opleiding in werkzaam zullen zijn.

De aanvrager verwijst voorts naar het artikel 'Cyber security sector zoekt in krappe arbeidsmarkt hoogopgeleid personeel' van VPN Gids (21 oktober 2021 met update 2 maart 2023). Uit het artikel volgt dat het aantal banen in de cybersecurity sector tussen 2013 en 2018 met ruim 22% is gestegen tot 142.000 arbeidsplaatsen en dat eind 2021 een enorme krapte in de arbeidsmarkt voor deze sector wordt verwacht. Het artikel spreekt ook de verwachting uit dat de sector tot 2025 per jaar gemiddeld met ongeveer 9% blijft groeien. Het merendeel van de vacatures (71,8%) in de sector is op hbo-niveau. Volgens het artikel is het aantal cybersecurity bedrijven de afgelopen vijf jaar verdubbeld. De vraag naar hogeropgeleide ethische hackers is in een halfjaar bijna verdubbeld: in april 2021 werd nog in 5,7% van de vacatures specifiek gevraagd om een ethical hacker, terwijl dit in september 2021 is opgelopen naar 9,2%. De commissie constateert dat de

arbeidsmarkt in de cybersecurity sector krap is (in het bijzonder op hbo-niveau) en dat deze krapte waarschijnlijk zal blijven aanhouden. Dit geeft blijk van een arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen opleiding.

De aanvrager doet daarnaast een beroep op de barometer 'ICT-beroepen: Barometer arbeidsmarkt' van het UWV (2021, p. 1) en het artikel 'De meest kansrijke beroepen van 2023' van Randstad (17 januari 2023) waarin security specialist en software engineer als meest kansrijke beroepen in de ICT-sector voor hoger opgeleiden worden omschreven. Het overzicht van 'Kansrijke beroepen' van het UWV (2022) omschrijft security specialisten en software testers eveneens als meest kansrijke beroepen in de ICT-sector. De 'IT arbeidsmarktmonitor 2021' van Hello Professionals (2022) stelt dat developer de meest gevraagde IT-functie van 2021 was. De commissie constateert dat voornoemde bronnen een positieve indicatie bieden van een arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen opleiding.

De aanvrager heeft in februari 2023 op de website Indeed.nl gezocht naar vacatures met de zoekterm 'cybersecurity' in de regio Apeldoorn. De zoekopdracht waarbij een straal van 50 kilometer rond Apeldoorn is gehanteerd heeft 94 resultaten opgeleverd. Dezelfde zoekopdracht waarbij een straal van 25 kilometer is gehanteerd leverde 28 resultaten op. Niet duidelijk is of gedurende één peilmoment of meerdere peilmomenten naar relevante vacatures is gezocht. Er is een link naar het zoekscherm meegeleverd. Het zoekscherm is ingesteld op vacatures met de zoekterm cybersecurity binnen een radius van 25 kilometer vanaf Apeldoorn. De commissie constateert dat de link naar het overzicht niet statisch is. Op het moment van eerste raadpleging door de commissie was het overzicht beperkt tot 21 vacatures en bij een volgende raadpleging tot 23 vacatures. Het overzicht van vacatures bevat een beperkt aantal vacatures dat aansluit bij het uitstroomprofiel van de beoogde opleiding. Afgestudeerden komen zowel wat betreft gevraagde werkervaring als wat betreft vereiste kennis in aanmerking voor functies als Cybersecurity Specialist/Ethical Hacker en Information Security Analist. De commissie constateert echter dat het merendeel van de vacatures om meerdere jaren relevante werkervaring op hbo- of wo-niveau vraagt of inhoudelijk onvoldoende aansluit op het profiel van de opleiding. Voor functies als Criminal Investigator of Digital Forensic Investigator wordt tenminste 5 jaar werkervaring vereist en een functie als Embedded Software Engineer Automotive sluit inhoudelijk niet aan op het profiel van de opleiding. De commissie is van mening dat op basis van de zoekopdracht op Indeed.nl geen arbeidsmarktbehoefte aan afgestudeerden van de beoogde Ad Cybersecurity kan worden vastgesteld.

De aanvrager verwijst ten slotte naar het arbeidsmarktonderzoek 'Doelmatigheidsonderzoek voor een voltijd Associate degree opleiding Cybersecurity' dat door Tien Organisatieadvies is uitgevoerd in opdracht van de aanvrager (2023). Het onderzoek bestaat uit twee deelonderzoeken. Het eerste deelonderzoek is gebaseerd op 10 interviews met (regionale) werkveldpartijen die hebben plaatsgevonden tussen oktober en december 2022. Het onderzoek bevat een overzicht van de namen en functies van de respondenten en de bedrijven waar zij voor werken. De gespreksleidraad die gebruikt is bij het afnemen van de interviews is ook in het arbeidsmarktonderzoek opgenomen.
Alle geïnterviewden zijn positief over de opleiding. De respondenten geven allemaal aan dat het belang van data/AI toeneemt en de sterke toename van cybercrime vraagt om hoogopgeleide securityspecialisten. De geïnterviewden geven aan het mbo-niveau te laag te achten voor de functies waarvoor zij personeel zoeken en verwachten dat een Ad de kloof tussen het mbo en hbo kan dichten. Daarbij geven de respondenten ook aan dat er een arbeidsmarktkrapte bestaat in het veld van cybersecurity. De geïnterviewden is gevraagd hoeveel afgestudeerden van de voorgenomen opleiding zij zouden willen aannemen. De respondenten hebben geschat hoeveel nieuwe medewerkers met het profiel van de beoogde hbo Ad Cybersecurity zij zouden willen aannemen. Zeven geïnterviewden geven aan een behoefte ter grootte van ongeveer 45 vacatures te hebben, maar geven geen tijdsindicatie waarin deze vacatures verwacht worden; twee geïnterviewden spreken over een behoefte ter grootte van gezamenlijk vier vacatures per jaar en

één geïnterviewde geeft aan dat het bedrijf te klein is om nieuwe medewerkers aan te nemen. De commissie acht het onderzoek valide en navolgbaar en constateert dat de respondenten relevante functies hebben en voor relevante bedrijven werken. De commissie is daarom van mening dat zij in staat zijn om een gezaghebbende uitspraak te doen over de arbeidsmarktbehoefte binnen hun organisaties. De commissie concludeert dat het onderzoek als geheel blijk geeft van een geringe regionale arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen opleiding.

Het tweede deelonderzoek in het arbeidsmarktonderzoek van Tien Organisatieadvies is gebaseerd op een online enquête onder 33 respondenten uit het werkveld. De bedrijven waar de 33 respondenten van de enquête voor werken en de vragen die aan hen zijn gesteld zijn in een bijlage van het onderzoeksrapport vermeld. De respondenten is wel gevraagd welke positie zij binnen hun organisatie bekleden, maar de antwoorden op deze vraag zijn niet in het dossier opgenomen. De vraagstelling suggereert echter dat de respondenten in staat zijn om gezaghebbende uitspraken over het aannamebeleid van de eigen organisatie te doen, aangezien bij de mogelijke antwoorden directie, bestuur, management, HRM en overig (met toelichting) zijn vermeld. De bedrijven die betrokken waren bij de interviews zijn niet bevraagd in de enquête. De respondenten is gevraagd of zij denken in de komende twee tot vijf jaar een behoefte te hebben aan nieuwe medewerkers binnen de eigen organisatie die de voorgenomen opleiding hebben gevolgd. 8 van de respondenten (24,2%) verwachten zeker een behoefte te hebben en 14 van de respondenten (42,4%) verwachten misschien een dergelijke behoefte te zullen hebben. Deze respondenten zien volgens het onderzoek een behoefte van minimaal 71 en maximaal 136 nieuwe medewerkers in de komende twee tot vijf jaar. In deze berekening is het antwoord 'meer dan 25' gerekend als 30 nieuwe medewerkers. Drie van de respondenten hebben aangegeven niet te weten hoeveel nieuwe medewerkers met de voorgenomen opleiding zij verwachten nodig te hebben. Uit het onderzoek blijkt dat er ongeveer 20 nieuwe medewerkers per jaar worden gezocht bij de respondenten. De commissie acht het arbeidsmarktonderzoek valide en ten dele navolgbaar omdat de aanvrager de bedrijven waar respondenten werkzaam voor zijn heeft vermeld. De door de aanvrager bijgeleverde lijst van bedrijven waar respondenten werkzaam voor zijn geeft duidelijk weer om welke bedrijven het gaat, maar er wordt niet expliciet gemaakt waarom de betrokken bedrijven relevant moeten worden geacht. De commissie acht het echter reëel dat de betrokken bedrijven mogelijk afgestudeerden van de voorgenomen opleiding zouden willen aannemen. De navolgbaarheid wordt in de ogen van de commissie enigszins beperkt door de afwezigheid van een lijst van functies van de respondenten, maar de vraagstelling in de meegeleverde voorbeeldenquête suggereert dat de respondenten in staat zijn om gezaghebbende uitspraken over het personeelsbeleid van de eigen organisatie te kunnen doen. Ook het ontbreken van een koppeling van de bedrijven, functies en benoemde behoefte beperkt de navolgbaarheid van de enquête enigszins. De commissie is van mening dat de enquête niettemin een positieve indicatie geeft van een arbeidsmarktbehoefte aan afgestudeerden van de voorgenomen opleiding.

De commissie concludeert op grond van het bovenstaande dat de aanvrager aannemelijk heeft gemaakt dat er een arbeidsmarktbehoefte bestaat aan de voorgenomen opleiding Cybersecurity.

Beoordeling maatschappelijke behoefte
De aanvrager onderbouwt de maatschappelijke behoefte aan de hand van de volgende bronnen: het 'Regeerakkoord 2017: Vertrouwen in de toekomst' (2017), het 'Coalitieakkoord 2021: Omzien naar elkaar, vooruitkijken naar de toekomst' (2021), de website van het Nationaal Cyber Security Centrum (www.ncsc.nl), de website van het Digital Trust Center (www.digitaltrustcenter.nl/over-het-digital-trust-center), het rapport 'Cybersecuritybeeld Nederland 2019' van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (2019), de website van het RIVM (www.rivm.nl/over-het-rivm/strategisch-programma-rivm/safety-en-security) en het themarapport 'Binnen zonder kloppen - Digitale weerbaarheid in het hoger onderwijs' van de Inspectie van het Onderwijs (2021).

De aanvrager verwijst ten eerste naar het 'Regeerakkoord 2017: Vertrouwen in de toekomst'

(2017, p. 3) en het 'Coalitieakkoord 2021: Omzien naar elkaar, vooruitkijken naar de toekomst' (2021, p. 33). In het Regeerakkoord van 2017 wordt onder meer aangegeven dat de toenmalige regering cybersecurity hoog op de maatschappelijke en politieke agenda had staan. Zo wordt er structureel 95 miljoen euro gereserveerd voor cybersecurity. De middelen worden onder andere ingezet voor de uitbreiding van personele capaciteit en ICT-voorzieningen. In het Regeerakkoord van 2017 wordt daarnaast aangegeven dat er een cybersecurityagenda zal worden opgesteld, dat onderzoek naar cybersecurity zal worden gestimuleerd en dat er betere voorlichtingscampagnes zullen komen. Het Coalitieakkoord van 2021 stelt dat in Europees verband zal worden ingezet op versterking van de samenwerking tussen lidstaten op het gebied van digitalisering, onder meer op mensgerichte inzet van kunstmatige intelligentie, digitale ethiek, ontwikkeling van digitale identiteit en cybersecurity en 'open source'.

De aanvrager verwijst tevens naar de website van het Nationaal Cyber Security Centrum (www.ncsc.nl) en de website van het Digital Trust Center (www.digitaltrustcenter.nl), organisaties die respectievelijk deel uitmaken van het Ministerie van Justitie en Veiligheid en het Ministerie van Economische Zaken en Klimaat. Beide organisaties zijn opgericht om de weerbaarheid van de Nederlandse samenleving in het digitale domein te vergroten. Het rapport 'Cybersecuritybeeld Nederland 2019' van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (2019) wordt door de aanvrager aangehaald om aan te geven dat de Nationaal Coördinator Terrorismebestrijding en Veiligheid er samen met zijn partners (zoals het Nationaal Cyber Security Centrum) ervoor beoogt te zorgen dat de Nederlandse vitale infrastructuur veilig is en blijft. Cybersecurity is hier een onderdeel van. Een ander voorbeeld van het belang van cybersecurity wordt gegeven op de website van het RIVM (www.rivm.nl), waar binnen het thema 'Safety and Security' binnen het eigen Strategisch Programma RIVM 2019-2022 (SPR) aan digitale informatieveiligheid wordt gewerkt.

De aanvrager stelt ten slotte dat ook binnen het hoger onderwijs aandacht bestaat voor IT security en cybersafety. In het themarapport 'Binnen zonder kloppen - Digitale weerbaarheid in het hoger onderwijs' van de Inspectie van het Onderwijs (2021, p. 5) wordt geconstateerd dat in de aanpak van en aandacht voor cybersecurity nog een te grote diversiteit bestaat. Bij sommige onderwijsinstellingen is cybersecurity een regulier aandachtspunt, terwijl dit bij andere onderwijsinstellingen nog nauwelijks het geval is. Deelname aan specialistische cybersafety platforms en netwerken is vaak vrijblijvend. De aanvrager wijst tevens op het belang van het Centrum voor Veiligheid en Digitalisering (CVD) dat in Apeldoorn is gevestigd. Het CVD is een initiatief van Saxion, de Politieacademie, de Universiteit Twente, de gemeente Apeldoorn, het Nederlands Instituut Publieke Veiligheid (NIPV) en Aventus in samenwerking met het Opleidings- en Kenniscentrum van de Koninklijke Marechaussee, de Koninklijke Landmacht en Apeldoorn IT, het netwerk van bedrijven en instellingen van IT professionals. Het CVD is een kennis- en innovatiehub waar plaats is voor onderwijs, onderzoek, netwerkbijeenkomsten en lezingen rondom het thema digitale veiligheid.

De commissie constateert op grond van het bovenstaande dat cybersecurity een beleidsprioriteit van de overheid vormt en dat ook binnen het hoger onderwijs een verhoogde aandacht bestaat voor cybersecurity. De beoogde opleiding is volledig gericht op cybersecurity en sluit hiermee aan op bovenstaande ontwikkelingen. De commissie is van mening dat de aanvrager hiermee een maatschappelijke behoefte aan de beoogde opleiding heeft aangetoond.

De commissie concludeert dat de aanvraag aansluit op een maatschappelijke en een arbeidsmarktbehoefte. De aanvraag voldoet aan criterium a in art. 4 lid 1 van de Regeling.

*Beoordeling criterium b*
Vanaf 13/03/2023 is op de website van de CDHO kennisgegeven van het voornemen van Saxion Hogeschool om de hbo Associate degree Cybersecurity in Apeldoorn aan te bieden. Hiermee is aan de instellingen voor hoger onderwijs de mogelijkheid gegeven om hun zienswijzen op dit voornemen kenbaar te maken. Er zijn geen zienswijzen ingediend.

De commissie stelt op basis van de afbakening die de aanvrager heeft aangeleverd vast wat het verwante aanbod van de aangevraagde opleiding is. Verwante opleidingen komen inhoudelijk sterk overeen en leiden op tot (min of meer) dezelfde beroepen (uitstroomprofiel(en)). Bij de inhoud wordt gekeken of de kennisgebieden en vaardigheden die in het curriculum van de voorgenomen opleiding zijn opgenomen overlap vertonen met de bestaande opleidingen. Verder worden de instroomdoelgroep en de onderwijsvariant (voltijd, deeltijd of duaal) meegewogen bij de afbakening.

De aanvrager acht de volgende hbo Ad-opleidingen "verwant" aan de voorgenomen opleiding: Cybersecurity (Hogeschool van Amsterdam, Hogeschool Utrecht) en Cyber Safety & Security (NHL Stenden Hogeschool). De aanvrager geeft aan dat de instroomgegevens van de Ad Cybersecurity van de Hogeschool Utrecht (HU) nog niet bekend zijn aangezien deze opleiding nog niet is gestart. Volgens de aanvrager is de aanvraag voor de voorgenomen opleiding op bestuursniveau afgestemd met de Hogeschool Utrecht en is er geen bezwaar tegen de komst van de beoogde Ad Cybersecurity. De aanvrager stelt tevens dat de eigen Ad Information Security waarvoor onlangs een positief besluit is ontvangen qua focus en aanpak dusdanig verschilt van de beoogde Ad Cybersecurity dat de opleidingen als niet verwant aan elkaar dienen te worden geacht. De aanvrager is van mening dat beide opleidingen elkaar aanvullen en versterken. De aanvrager geeft aan de mogelijk verwante onbekostigde Ad-opleiding Security Management van LOI Hogeschool niet te hebben betrokken omdat hier geen instroom van bekend is. De aanvrager gebruikt in het dossier de term "verwant", hetgeen door de commissie begrepen wordt als vergelijkbaar met de door de commissie gebruikte term "sterk verwant".

De commissie is van mening dat de Ad-opleidingen Cybersecurity (Hogeschool van Amsterdam en Hogeschool Utrecht) en Cyber Safety & Security (NHL Stenden Hogeschool) sterk verwant zijn aan de voorgenomen opleiding. Anders dan de aanvrager acht de commissie de Ad Information Security (Hogeschool Rotterdam en Saxion Hogeschool) sterk verwant aan de beoogde Ad Cybersecurity. De aanvrager stelt dat de focus van de Ad Cybersecurity verschilt van die van de Ad Information Security in die zin dat de Ad Cybersecurity zich meer richt op wat er zich in de digitale buitenwereld (cyberspace) afspeelt: de opleiding is gericht op de bescherming van digitale systemen, netwerken, apparaten en gegevens tegen cyberdreigingen, zoals hacken, malware, phishing en andere vormen van cyberaanvallen. De Ad Information Security is gericht op bescherming van alle soorten gevoelige en vertrouwelijke informatie tegen ongeoorloofde toegang, gebruik, openbaarmaking, verstoring, wijziging of vernietiging daarvan. De commissie constateert dat de instroomeisen van beide opleidingen identiek zijn: studenten kunnen instromen met een havo-, vwo- of mbo4-diploma. De commissie heeft verder de inhoud van de beide opleidingen met elkaar vergeleken en constateert dat in de beoogde Ad Cybersecurity thema's als Operating Systems, Network Infrastructure & Security, Coding/scripting, Ethical Hacking, Web Applications, Security Monitoring, Security Governance en Threat Intelligence aan bod komen. In de Ad Information Security wordt aandacht besteed aan de thema's Security Management, Risiciobepaling Informatie(voorziening), Information Security en IT Security, Risicoanalyse en Securitymaatregelen ontwerpen en Security realiseren. De commissie acht de inhoudelijke verschillen niet dusdanig groot dat de opleidingen niet als sterk verwant aan elkaar kunnen worden beschouwd. Ook de beroepen waarvoor afgestudeerden in aanmerking komen vertonen een sterke overlap. Afgestudeerden van de Ad Cybersecurity komen in aanmerking voor functies als Security Consultant, Security Architect, Pentester, Information Security Officer en Ethical Hacker. Afgestudeerden van de Ad Information Security komen in aanmerking voor functies als Security Officer, Junior Security Manager, Threathunter en Operational Security Manager. De

commissie is van mening dat afgestudeerden van beide opleidingen voor min of meer dezelfde functies in aanmerking komen.
Daarnaast is de commissie van mening dat de Ad IT Security Management (Hogeschool INHOLLAND) eveneens sterk verwant is aan de voorgenomen opleiding. De commissie acht deze opleiding sterk verwant omdat zij nèt als de Ad Information Security vrijwel identiek is aan de beoogde Ad Cybersecurity. Ook deze opleiding kent identieke instroomeisen, een sterke inhoudelijke overlap en afgestudeerden komen in aanmerking voor min of meer dezelfde functies als afgestudeerden van de Ad Cybersecurity. De commissie merkt op dat de Ad-opleidingen Cybersecurity van de Hogeschool Utrecht, Cybersafety & Security, Information Security en IT Security Management nog niet zijn gestart en de instroomgegevens derhalve niet beschikbaar zijn.

De commissie acht de volgende hbo Ad-opleidingen aanverwant aan de voorgenomen opleiding: AD-ICT (Fontys Hogescholen), ICT (Zuyd Hogeschool), ICT Service Management (Christelijke Hogeschool Ede, Fontys Hogescholen en Hogeschool Rotterdam), ICT-Beheer (NHL Stenden Hogeschool), Informatica (Avans Hogeschool) en IT Service Management (Hogeschool INHOLLAND en NHL Stenden Hogeschool). De commissie overweegt hierbij dat de aandacht die deze opleidingen besteden aan cybersecurity ten dele overlapt met de voorgenomen opleiding, dat de opleidingen dezelfde instroomdoelgroep bedienen en dat afgestudeerden deels voor vergelijkbare functies (zoals ethical hacker, pentester en security consultant) in aanmerking komen. De aanverwante opleidingen kennen inhoudelijk een bredere scope en zijn niet specifiek gericht op cybersecurity.

De aanvrager heeft een overzicht geleverd van de instroom in verwante bekostigde opleidingen. De commissie neemt de instroom in de sterk verwante onbekostigde Ad-opleiding Security Management van LOI niet mee in de onderstaande overweging omdat deze bij de commissie niet bekend is. De instroom in het sterk verwante en aanverwante aanbod is in de afgelopen vijf jaar licht gestegen (zie Tabel 4).

Tabel 4. Instroom eerstejaarsstudenten in verwant bekostigd onderwijsaanbod

| **Opleiding** | **Instelling** | **'17-'18** | | **'18-'19** | | **'19-'20** | | **'20-'21** | | **'21-'22** | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ***VT*** | ***DT*** | ***VT*** | ***DT*** | ***VT*** | ***DT*** | ***VT*** | ***DT*** | ***VT*** | ***DT*** |
| Ad Cybersecurity (80156) | Hogeschool van Amsterdam (28DN), Amsterdam | | | | | 53 | | 81 | | 86 | |
| Ad AD-ICT (80152) | Fontys Hogeschool (30GB), Eindhoven | | | | | | | 27 | 27 | 44 | 62 |
| | Fontys Hogeschool (30GB), Tilburg | | | | | 21 | | 55 | | 48 | |
| Ad ICT (80132) | Zuyd Hogeschool (25JX), Heerlen | 100 | 10 | 92 | | 54 | | 88 | | 67 | 2 |
| Ad ICT Service Management (80083) | Christelijke Hogeschool Ede (25BA), Ede | | | | 11 | | 9 | | 9 | | 6 |
| | Fontys Hogeschool (30GB), Eindhoven | | 20 | | 26 | | 20 | | 3 | | 2 |
| | Hogeschool Rotterdam (22OJ), Rotterdam | 77 | 41 | 68 | 28 | 50 | 26 | 45 | 25 | 30 | 27 |
| Ad ICT-Beheer (80071) | Christelijke Hogeschool Windesheim (01VU), Zwolle | | 13 | | 1 | | | | | | |
| | NHL Stenden Hogeschool (31FR), Emmen | 10 | | 8 | | 5 | | 13 | | 13 | |
| Ad Informatica (80075) | Avans Hogeschool (07GR), 's-Hertogenbosch | 17 | | 39 | | 38 | | 30 | | 24 | |
| | Avans Hogeschool (07GR), Breda | | | | | | 25 | | 39 | | 22 |
| | Avans Hogeschool (07GR), Roosendaal | | | 27 | | 25 | | 28 | | 25 | |
| Ad IT Service Management (80024) | Hogeschool INHOLLAND (27PZ), Diemen | 15 | | 15 | | 16 | 20 | 30 | 10 | 23 | 8 |
| | NHL Stenden Hogeschool (31FR), Leeuwarden | 5 | | 4 | | 7 | 6 | 10 | 6 | 15 | 12 |
| ***Totaal*** | | ***224*** | ***84*** | ***253*** | ***66*** | ***216*** | ***106*** | ***326*** | ***119*** | ***289*** | ***141*** |

*Bron: DUO*

De aanvrager heeft een prognose gemaakt van de instroom in de voorgenomen opleiding op grond van een instroomenquête welke onderdeel is van het arbeidsmarktonderzoek 'Doelmatigheidsonderzoek voor een voltijd Associate degree opleiding Cybersecurity' van Tien Organisatieadvies. De enquête is uitgevoerd onder havo- en mbo-4-leerlingen in het verzorgingsgebied van de aanvrager. De aanvrager verwacht dat jaarlijks 25 studenten zullen instromen. De commissie acht deze prognose realistisch.

Als de instroom in de bestaande opleidingen en de verwachte instroom in de voorgenomen hbo Associate degree Cybersecurity wordt afgezet tegen de behoefte die bij criterium a aannemelijk is gemaakt, blijkt dat er geen ruimte is om deze opleiding binnen het bekostigde domein vorm te geven. De kern van de overweging berust op de constatering dat de beoogde opleiding dusdanig sterk verwant is voor wat betreft inhoud, instroomdoelgroep, opleidingsvorm en arbeidsmarktprofiel aan de nog te starten Ad Information Security dat geen ruimte in de regio rondom Apeldoorn bestaat om deze opleiding aan het bestaande aanbod toe te voegen. De commissie overweegt daarnaast dat een relatief groot aantal verwante opleidingen op korte termijn van start zal gaan en dat nog onduidelijk is hoe deze opleidingen zich zullen ontwikkelen.

Vestiging van de opleiding in Apeldoorn heeft naar mening van de commissie negatief effect op de landelijke spreiding van het onderwijsaanbod omdat de sterk verwante Ad Information Security eveneens in Apeldoorn zal worden aangeboden. De commissie merkt op dat de verwachte instroom in de Ad Information Security 40 studenten voor de voltijdvariant bedraagt en 35 studenten voor de deeltijdvariant. De commissie acht de kans reëel dat de Ad-opleidingen Cybersecurity en Information Security instroom bij elkaar zullen wegnemen. Deze ontwikkeling acht de commissie niet doelmatig.

De commissie concludeert dat er geen ruimte in het landelijk aanbod bestaat om de hbo Associate degree Cybersecurity te realiseren. De aanvraag voldoet niet aan criterium b in art. 4 lid 1 van de Regeling.

Gelet op het vorenstaande adviseert de Commissie Doelmatigheid Hoger Onderwijs u om negatief te besluiten op het voorliggende verzoek.

*Advies aan de NVAO over de naamkeuze en Croho indeling*
De commissie heeft geconstateerd dat de voorgestelde naam van de opleiding passend is gelet op de namen van verwante opleidingen. Daarnaast heeft de commissie geconstateerd dat de aanvrager de hbo Associate degree Cybersecurity in het Croho onderdeel Techniek wil indelen. Dit voorstel sluit aan op de indeling van verwante bestaande opleidingen.

De NVAO ontvangt dit advies, zodat zij dit kan opnemen in het informatiedossier voor het panel ten behoeve van de toets nieuwe opleiding.

De Commissie Doelmatigheid Hoger Onderwijs

drs. P.M.M. Rullmann
*Voorzitter CDHO*

**Bijlage:**

**Beoordelingskader macrodoelmatigheid nieuwe opleiding of nevenvestiging**
Aan de hand van de in de Regeling macrodoelmatigheid hoger onderwijs van 20 juni 2018 genoemde voorwaarden worden voornemens tot het verzorgen van een nieuwe opleiding beoordeeld op doelmatigheid. Een nieuwe opleiding kan volgens artikel 4 van deze Regeling alleen doelmatig worden geacht indien het voornemen voldoet aan de criteria a en b.

Volgens criterium a heeft het instellingsbestuur aangetoond dat er behoefte bestaat aan de nieuwe opleiding of nevenvestiging, zijnde overwegend een arbeidsmarktbehoefte, dan wel een overwegend maatschappelijke behoefte in combinatie met een arbeidsmarktbehoefte, dan wel een overwegend wetenschappelijke behoefte in combinatie met een arbeidsmarktbehoefte.

Volgens criterium b dient het instellingsbestuur aan te tonen dat in de behoefte die bij criterium a is aangetoond niet door het bestaande opleidingenaanbod wordt voorzien.

*Advies aan de NVAO over naamkeuze en Croho indeling*
In de Toelichting op de Regeling is aangegeven dat de CDHO ook een rol heeft bij de beoordeling van de voorgestelde naam en voertaal van de opleiding en bij de voorgestelde positionering in het Croho.

Wat betreft de opleidingsnaam: de CDHO kijkt of de voorgestelde naam van de opleiding passend is, gelet op de namen van verwante opleidingen. Daarbij is het uitgangspunt dat sterk op elkaar lijkende opleidingen dezelfde naam krijgen, om de transparantie van het opleidingenaanbod voor studiekiezers en werkgevers te borgen. In het Croho kan ook een internationale (Engelse) naam worden geregistreerd. Dit onderdeel van het CDHO advies is niet gericht aan de Minister van OCW, maar aan de NVAO. Het panel van de NVAO toetst of de naamkeuze gerechtvaardigd is gelet op de inhoud van de opleiding en de namen van vergelijkbare opleidingen (artikel 5.7, vierde lid, onderdeel a, van de WHW).

Wat betreft de positie in het Croho: de CDHO kijkt of de voorgestelde indeling in het Croho passend is, gelet op de indeling van verwante opleidingen. Daarbij is het uitgangspunt dat sterk op elkaar lijkende opleidingen in hetzelfde Croho onderdeel worden geregistreerd, om de transparantie van het opleidingenaanbod voor studiekiezers en werkgevers te borgen. Dit onderdeel van het CDHO advies is niet gericht aan de Minister van OCW, maar aan de NVAO. Het panel van de NVAO toetst of de voorgestelde indeling in het Croho aansluit bij de ordening van verwante opleidingen.